ESET NOD32 ANTIVIRUS 10

User Guide

(intended for product version 10.0 and higher)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista

Click here to download the most recent version of this document

ESET **NOD32 ANTIVIRUS**

Copyright ©2016 by ESET, spol. s r. o.
ESET NOD32 Antivirus was developed by ESET, spol. s r. o.
For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r. o. reserves the right to change any of the described application software without prior notice.

Worldwide Customer Support: www.eset.com/support

REV. 9/28/2016

Contents

1. ESET NOD32 Antivirus.....5
1.1 What's new in version 10.....5
1.2 Which product do I have?.....6
1.3 System requirements.....7
1.4 Prevention.....7
2. Installation.....9
2.1 Live installer.....9
2.2 Offline installation.....10
2.2.1 Advanced settings.....11
2.3 Common installation problems.....11
2.4 Product activation.....11
2.5 Entering your License key.....12
2.6 Upgrading to a more recent version.....12
2.7 First scan after installation.....13
3. Beginner's guide.....14
3.1 The main program window.....14
3.2 Updates.....16
4. Working with ESET NOD32 Antivirus.....18
4.1 Computer protection.....19
4.1.1 Antivirus.....20
4.1.1.1 Real-time file system protection.....21
4.1.1.1.1 Additional ThreatSense parameters.....22
4.1.1.1.2 Cleaning levels.....22
4.1.1.1.3 When to modify real-time protection configuration.....23
4.1.1.1.4 Checking real-time protection.....23
4.1.1.1.5 What to do if real-time protection does not work.....23
4.1.1.2 Computer scan.....23
4.1.1.2.1 Custom scan launcher.....24
4.1.1.2.2 Scan progress.....26
4.1.1.2.3 Scan profiles.....27
4.1.1.2.4 Computer scan log.....27
4.1.1.3 Idle-state scanning.....27
4.1.1.4 Startup scan.....27
4.1.1.4.1 Automatic startup file check.....28
4.1.1.5 Exclusions.....28
4.1.1.6 ThreatSense parameters.....29
4.1.1.6.1 Cleaning.....34
4.1.1.6.2 File extensions excluded from scanning.....34
4.1.1.7 An infiltration is detected.....35
4.1.1.8 Document protection.....37
4.1.2 Removable media.....37
4.1.3 Device control.....38
4.1.3.1 Device control rules editor.....39
4.1.3.2 Adding Device control rules.....40
4.1.4 Host-based Intrusion Prevention System (HIPS).....41
4.1.4.1 Advanced setup.....43
4.1.4.2 HIPS interactive window.....44
4.1.4.3 Potential ransomware behavior detected.....45
4.1.5 Gamer mode.....45
4.2 Internet protection.....46
4.2.1 Web access protection.....46
4.2.1.1 Basic.....47
4.2.1.2 Web protocols.....47
4.2.1.3 URL address management.....48
4.2.2 Email client protection.....49
4.2.2.1 Email clients.....49
4.2.2.2 Email protocols.....50
4.2.2.3 Alerts and notifications.....51
4.2.2.4 Integration with email clients.....51
4.2.2.4.1 Email client protection configuration.....51
4.2.2.5 POP3, POP3S filter.....52
4.2.3 Protocol filtering.....52
4.2.3.1 Web and email clients.....53
4.2.3.2 Excluded applications.....53
4.2.3.3 Excluded IP addresses.....54
4.2.3.3.1 Add IPv4 address.....54
4.2.3.3.2 Add IPv6 address.....54
4.2.3.4 SSL/TLS.....55
4.2.3.4.1 Certificates.....56
4.2.3.4.1.1 Encrypted network traffic.....56
4.2.3.4.2 List of known certificates.....56
4.2.3.4.3 List of SSL/TLS filtered applications.....57
4.2.4 Anti-Phishing protection.....57
4.3 Updating the program.....58
4.3.1 Update settings.....61
4.3.1.1 Update profiles.....62
4.3.1.2 Advanced update setup.....63
4.3.1.2.1 Update mode.....63
4.3.1.2.2 HTTP Proxy.....63
4.3.2 Update rollback.....64
4.3.3 How to create update tasks.....65
4.4 Tools.....65
4.4.1 Tools in ESET NOD32 Antivirus.....66
4.4.1.1 Log files.....67
4.4.1.1.1 Log files.....68
4.4.1.2 Running processes.....69
4.4.1.3 Protection statistics.....70
4.4.1.4 Watch activity.....71
4.4.1.5 ESET SysInspector.....71
4.4.1.6 Scheduler.....72
4.4.1.7 ESET SysRescue.....73
4.4.1.8 ESET LiveGrid®.....74
4.4.1.8.1 Suspicious files.....75
4.4.1.9 Quarantine.....75
4.4.1.10 Proxy server.....76
4.4.1.11 Email notifications.....77
4.4.1.11.1 Message format.....78
4.4.1.12 Select sample for analysis.....78
4.4.1.13 Microsoft Windows® update.....79

4.5 User interface 79
4.5.1 User interface elements 79
4.5.2 Alerts and notifications 80
4.5.2.1 Advanced setup 81
4.5.3 Access setup 82
4.5.4 Program menu 83

5. Advanced user 84

5.1 Profile manager 84
5.2 Keyboard shortcuts 84
5.3 Diagnostics 85
5.4 Import and export settings 86
5.5 ESET SysInspector 86
5.5.1 Introduction to ESET SysInspector 86
5.5.1.1 Starting ESET SysInspector 87
5.5.2 User Interface and application usage 87
5.5.2.1 Program Controls 87
5.5.2.2 Navigating in ESET SysInspector 89
5.5.2.2.1 Keyboard shortcuts 90
5.5.2.3 Compare 91
5.5.3 Command line parameters 92
5.5.4 Service Script 93
5.5.4.1 Generating Service script 93
5.5.4.2 Structure of the Service script 93
5.5.4.3 Executing Service scripts 96
5.5.5 FAQ 97
5.5.6 ESET SysInspector as part of ESET NOD32 Antivirus 98
5.6 Command Line 98

6. Glossary 101

6.1 Types of infiltration 101
6.1.1 Viruses 101
6.1.2 Worms 101
6.1.3 Trojans 101
6.1.4 Rootkits 102
6.1.5 Adware 102
6.1.6 Spyware 102
6.1.7 Packers 103
6.1.8 Potentially unsafe applications 103
6.1.9 Potentially unwanted applications 103
6.2 ESET Technology 105
6.2.1 Exploit Blocker 105
6.2.2 Advanced Memory Scanner 105
6.2.3 ESET LiveGrid® 106
6.2.4 Java Exploit Blocker 106
6.2.5 Script-Based Attacks Protection 106
6.2.6 Ransomware Protection 106
6.3 Email 107
6.3.1 Advertisements 107
6.3.2 Hoaxes 107
6.3.3 Phishing 108

7. Common Questions 109

7.1 How to update the ESET NOD32 Antivirus 109
7.2 How to remove a virus from my PC 109
7.3 How to create a new task in Scheduler 110
7.4 How to schedule a weekly computer scan 110

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus represents a new approach to truly integrated computer security. The most recent version of the ESET LiveGrid® scanning engine utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software that might endanger your computer.

ESET NOD32 Antivirus is a complete security solution that combines maximum protection and a minimal system footprint. Our advanced technologies use artificial intelligence to prevent infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other threats without hindering system performance or disrupting your computer.

Features and benefits

Redesigned user interface	The user interface in version 10 has been significantly redesigned and simplified based on the results of usability testing. All GUI wording and notifications have been carefully reviewed and the interface now provides support for right-to-left languages such as Hebrew and Arabic. **Online help** is now integrated into ESET NOD32 Antivirus and offers dynamically updated support content.
Antivirus and antispyware	Proactively detects and cleans more known and unknown viruses, worms, trojans and rootkits. **Advanced heuristics** flags even never-before-seen malware, protecting you from unknown threats and neutralizing them before they can do any harm. **Web access protection** and **Anti-Phishing** works by monitoring communication between web browsers and remote servers (including SSL). **Email client protection** provides control of email communication received through the POP3(S) and IMAP(S) protocols.
Regular updates	Regularly updating the virus signature database and program modules is the best way to ensure the maximum level of security on your computer.
ESET LiveGrid® (Cloud-powered Reputation)	You can check the reputation of running processes and files directly from ESET NOD32 Antivirus.
Device control	Automatically scans all USB flash drives, memory cards and CDs/DVDs. Blocks removable media based on the type of media, manufacturer, size and other attributes.
HIPS functionality	You can customize the behavior of the system in greater detail; specify rules for the system registry, active processes and programs, and fine-tune your security posture.
Gamer mode	Postpones all pop-up windows, updates or other system-intensive activities to conserve system resources for gaming and other full-screen activities.

A license needs to be active in order for features of ESET NOD32 Antivirus to be operational. It is recommended that you renew your license several weeks before the license for ESET NOD32 Antivirus expires.

1.1 What's new in version 10

ESET NOD32 Antivirus version 10 features the following improvements:

- **High performance and low system impact** – Version 10 is designed for efficient use of system resources, allowing you to enjoy your computer's performance while defending against new types of threats.
- **Windows 10 compatibility** – ESET fully supports Microsoft Windows 10.

For more details about new features in ESET NOD32 Antivirus please read the following ESET Knowledgebase article: What's new in Home product version 10?

1.2 Which product do I have?

ESET offers multiple layers of security with new products from powerful and fast antivirus solution to all-in-one security solution with minimal system footprint:

- **ESET NOD 32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security**
- **ESET Smart Security Premium**

To determine which product you have installed open the main program window (see the Knowledgebase article) and you will see the name of the product at the top of the window (header).

The table below details features available in each specific product.

	ESET NOD 32 Antivirus	ESET Internet Security	ESET Smart Security	ESET Smart Security Premium
Antivirus	✔	✔	✔	✔
Antispyware	✔	✔	✔	✔
Exploit Blocker	✔	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Antispam		✔	✔	✔
Personal Firewall		✔	✔	✔
Home Network protection		✔	✔	✔
Webcam Protection		✔	✔	✔
Network Attack Protection		✔	✔	✔
Botnet Protection		✔	✔	✔
Banking & Payment Protection		✔	✔	✔
Parental Control		✔	✔	✔
Anti-Theft			✔	✔
ESET Password Manager				✔
ESET Secure Data				✔

NOTE
Some of the products above may not be available for your language.

1.3 System requirements

Your system should meet the following hardware and software requirements for ESET NOD32 Antivirus to perform optimally:

Processors Supported

Intel® or AMD x86-x64

Supported Operating Systems

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 64-bit

NOTE
ESET Anti-Theft does not support Microsoft Windows Home Servers.

1.4 Prevention

When you work with your computer, and especially when you browse the Internet, please keep in mind that no antivirus system in the world can completely eliminate the risk of infiltrations and attacks. To provide maximum protection and convenience, it is essential that you use your antivirus solution correctly and adhere to several useful rules:

Update regularly

According to statistics from ThreatSense, thousands of new, unique infiltrations are created each day in order to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at the ESET Research Lab analyze these threats on a daily basis and prepare and release updates in order to continually improve the level of protection for our users. To ensure the maximum effectiveness of these updates it is important that updates are configured properly on your system. For more information on how to configure updates, see the Update setup chapter.

Download security patches

The authors of malicious software often exploit various system vulnerabilities in order to increase the effectiveness of spreading malicious code. With this in mind, software companies watch closely for any vulnerabilities in their applications to appear and release security updates to eliminate potential threats on a regular basis. It is important to download these security updates as they are released. Microsoft Windows and web browsers such as Internet Explorer are two examples of programs for which security updates are released on a regular schedule.

Back up important data

Malware writers usually do not care about users' needs, and the activity of malicious programs often leads to total malfunction of an operating system and the loss of of important data. It is important to regularly back up your important and sensitive data to an external source such as a DVD or external hard drive. This will make it far easier and faster to recover your data in the event of system failure.

Regularly scan your computer for viruses

Detection of more known and unknown viruses, worms, trojans and rootkits are handled by the Real-time file system protection module. This means that every time you access or open a file, it is scanned for a malware activity. We recommend that you run a full Computer scan at least once a month because malware signatures may vary and the virus signature database updates itself each day.

Follow basic security rules

This is the most useful and most effective rule of all – always be cautious. Today, many infiltrations require user intervention in order to be executed and distributed. If you are cautious when opening new files, you will save considerable time and effort that would otherwise be spent cleaning infiltrations. Here are some useful guidelines:

- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe Internet websites.
- Be cautious when opening email attachments, particularly those from mass-mailed messages and messages from unknown senders.
- Don't use an Administrator account for everyday work on your computer.

2. Installation

There are several methods for installing ESET NOD32 Antivirus on your computer. Installation methods may vary depending on country and means of distribution:

- Live installer can be downloaded from the ESET website. The installation package is universal for all languages (choose a desired language). Live installer itself is a small file; additional files required to install ESET NOD32 Antivirus will be downloaded automatically.

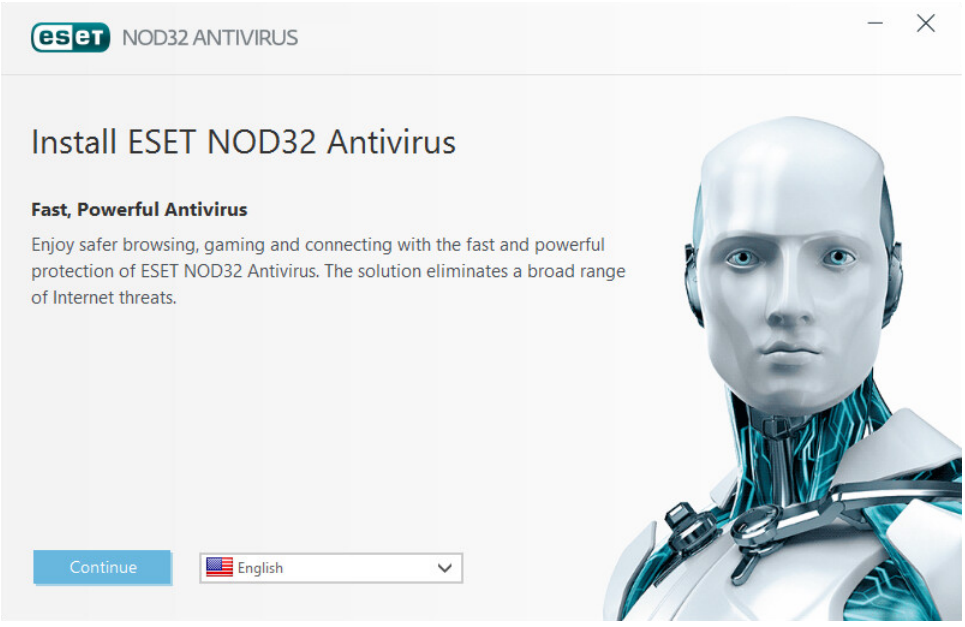
- Offline installation – This type of installation is used when installing from a product CD/DVD. It uses an *.exe* file that is larger than the Live installer file and does not require an internet connection or additional files for the completion of installation.

IMPORTANT
Make sure that no other antivirus programs are installed on your computer before you install ESET NOD32 Antivirus. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our ESET Knowledgebase article for a list of uninstaller tools for common antivirus software (available in English and several other languages).

2.1 Live installer

Once you have downloaded the *Live installer* installation package, double-click the installation file and follow the step-by-step instructions in the installer window.

IMPORTANT
For this type of installation you must be connected to Internet.


NOD32 ANTIVIRUS
Install ESET NOD32 Antivirus
Fast, Powerful Antivirus
Enjoy safer browsing, gaming and connecting with the fast and powerful protection of ESET NOD32 Antivirus. The solution eliminates a broad range of Internet threats.
Continue
English

Select your desired language from the drop-down menu and click **Continue**. Allow a few moments for installation files to download.

After you accept the **End-User License Agreement**, you will be prompted to configure **ESET LiveGrid®**. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new threats in order to protect our customers. The system allows you to submit new threats to the ESET Research Lab where they are analyzed, processed and added to the virus signature database.

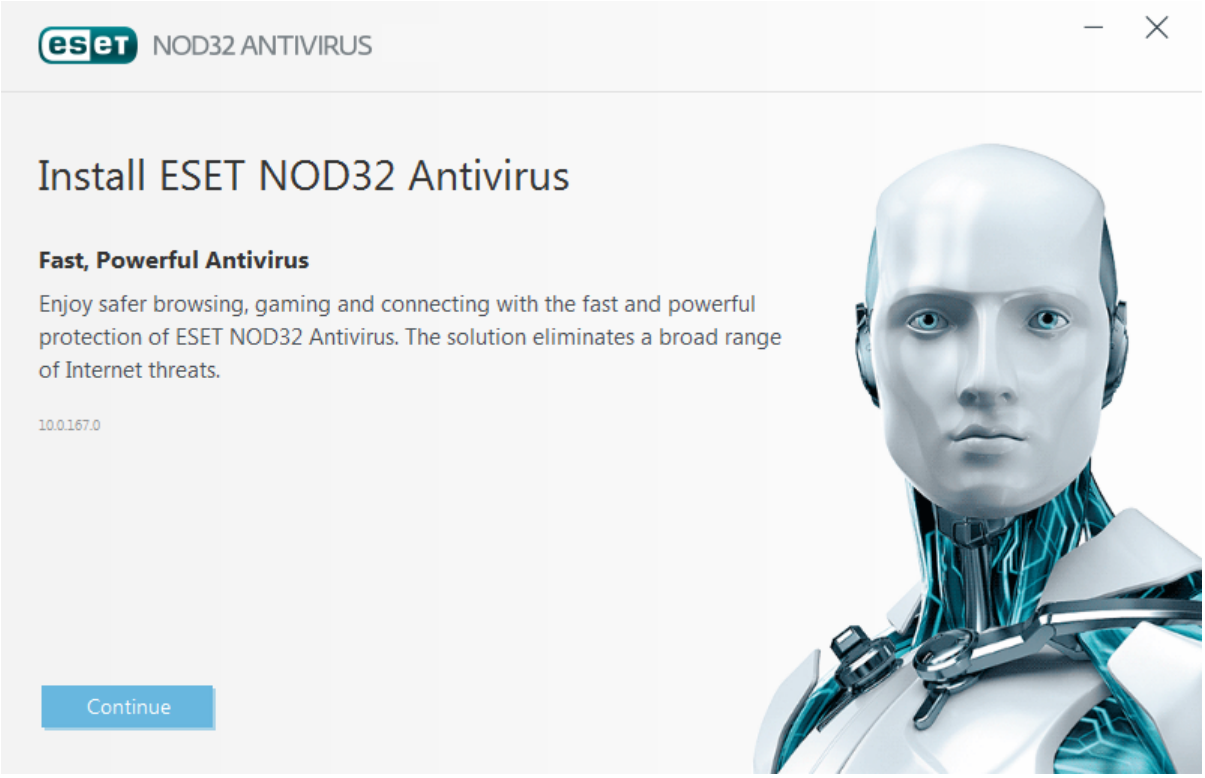
By default, **Enable ESET LiveGrid® feedback system (recommended)** is selected, which will activate this feature.

The next step in the installation process is to configure detection of potentially unwanted applications. Potentially unwanted applications are not necessarily malicious, but can negatively affect the behavior of your operating system. See the Potentially unwanted applications chapter for more details.

Click **Install** to start the installation process.

2.2 Offline installation

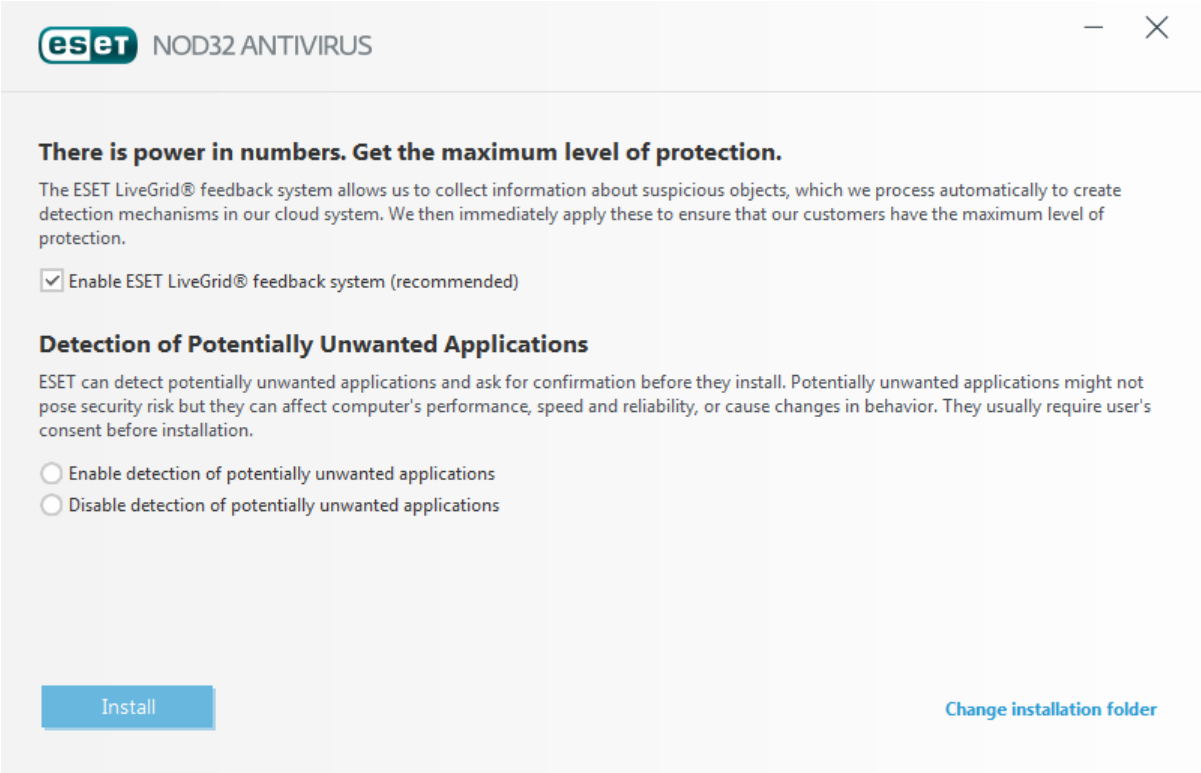
Once you launch the offline installation (.exe), the installation wizard will guide you through the setup process.


NOD32 ANTIVIRUS
Install ESET NOD32 Antivirus
Fast, Powerful Antivirus
Enjoy safer browsing, gaming and connecting with the fast and powerful protection of ESET NOD32 Antivirus. The solution eliminates a broad range of Internet threats.
10.0.167.0
Continue

First, the program checks to see if a newer version of ESET NOD32 Antivirus is available. If a newer version is found you will be notified in the first step of the installation process. If you select **Download and install new version**, the new version will be downloaded and installation will continue. This check box is visible only when there is a version newer than the version you are installing available.

Next, the End-User License Agreement will be displayed. Please read the agreement and click **Accept** to acknowledge your acceptance of the End-User License Agreement. After you accept, installation will continue.

For more instructions about installation steps, **ESET LiveGrid®** and **Detection of potentially unwanted applications**, follow the instructions in the aforementioned section (see "Live installer").


NOD32 ANTIVIRUS
There is power in numbers. Get the maximum level of protection.
The ESET LiveGrid® feedback system allows us to collect information about suspicious objects, which we process automatically to create detection mechanisms in our cloud system. We then immediately apply these to ensure that our customers have the maximum level of protection.
Enable ESET LiveGrid® feedback system (recommended)
Detection of Potentially Unwanted Applications
ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications
Install
Change installation folder

2.2.1 Advanced settings

After selecting **Change installation folder**, you will be prompted to select a location for the installation. By default, the program installs to the following directory:

C:\Program Files\ESET\ESET NOD32 Antivirus

Click **Browse** to change this location (not recommended).

To complete the next installation steps, **ESET LiveGrid®** and **Detection of potentially unwanted applications**, follow the instructions in the Live installer section (see "Live installer").

Click **Continue** and then **Install** to complete installation.

2.3 Common installation problems

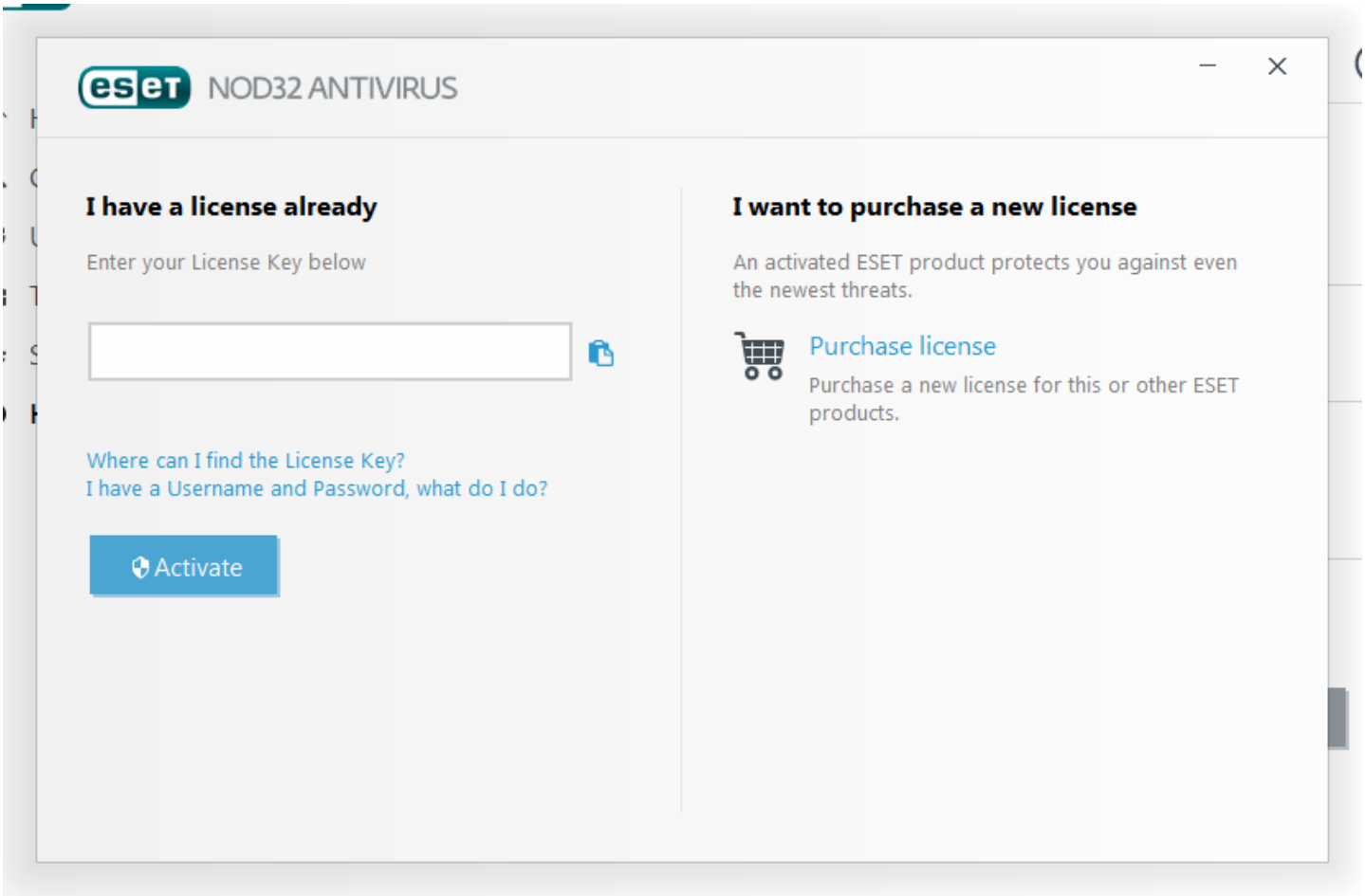
If problems occur during installation, see our list of common installation errors and resolutions to find a solution to your problem.

2.4 Product activation

After the installation is complete, you will be prompted to activate your product.

There are several methods available to activate your product. Availability of a particular activation scenario in the activation window may vary depending on country and means of distribution (CD/DVD, ESET web page, etc.):

- If you purchased a retail boxed version of the product, activate your product using a **License Key**. The License Key is usually located inside or on the back side of the product package. The License Key must be entered as supplied for activation to be successful. License Key – a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX or XXXX-XXXXXXXX which is used for identification of the license owner and for activation of the license.
- If you would like to evaluate ESET NOD32 Antivirus before making a purchase, select **Free trial license**. Enter your email address and country to activate ESET NOD32 Antivirus for a limited time. Your test license will be emailed to you. Trial licenses can only be activated once per customer.
- If you do not have a license and would like to buy one, click **Purchase license**. This will redirect you to the website of your local ESET distributor.


NOD32 ANTIVIRUS
I have a license already
Enter your License Key below
Where can I find the License Key?
I have a Username and Password, what do I do?
Activate
I want to purchase a new license
An activated ESET product protects you against even the newest threats.
Purchase license
Purchase a new license for this or other ESET products.

2.5 Entering your License key

Automatic updates are important for your security. ESET NOD32 Antivirus will only receive updates once activated using your **License Key**.

If you did not enter your License Key after installation, your product will not be activated. You can change your license in the main program window. To do so, click **Help and support** > **Activate License** and enter the license data you received with your ESET security product into the Product activation window.

When entering your **License key**, it is important to type it exactly as it is written:

- Your License Key is a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and activation of the license.

We recommend that you copy and past your License Key from your registration email to ensure accuracy.

2.6 Upgrading to a more recent version

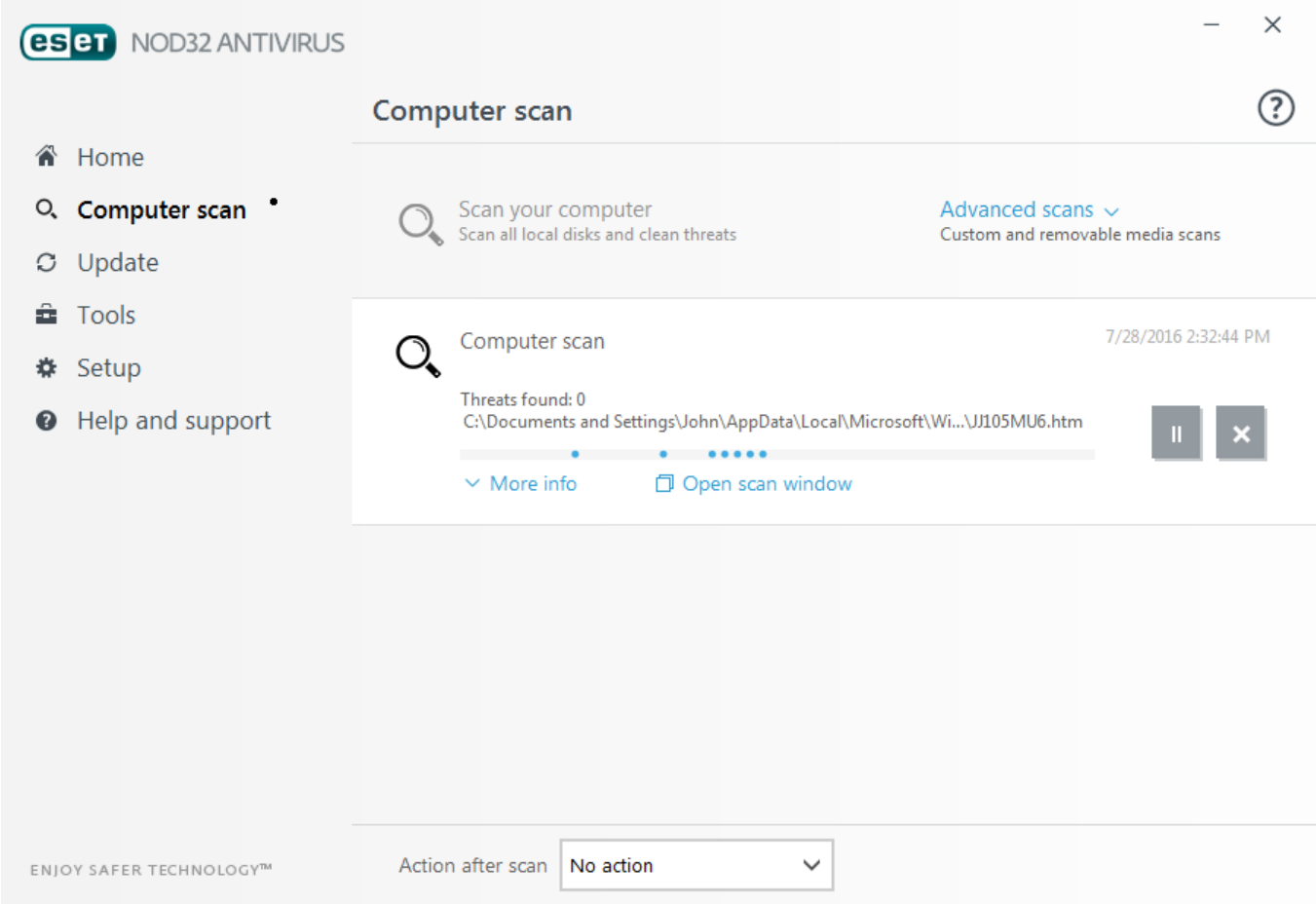
New versions of ESET NOD32 Antivirus are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules. Upgrading to a more recent version can be accomplished in several ways:

1. Automatically, by means of a program update.
   Since the program upgrade is distributed to all users and may have an impact on certain system configurations, it is issued after a long testing period to ensure functionality with all possible system configurations. If you need to upgrade to a newer version immediately after its release, use one of the methods below.
2. Manually, in the main program window by clicking **Check for updates** in the **Update** section.
3. Manually, by downloading and installing a more recent version over the previous one.

2.7 First scan after installation

After installing ESET NOD32 Antivirus, a computer scan will start automatically after first successful update in order to check for malicious code.

You can also start a computer scan manually from the main program window by clicking **Computer scan** > **Scan your computer**. For more information about computer scans, see the section Computer scan.



3. Beginner's guide

This chapter provides an initial overview of ESET NOD32 Antivirus and its basic settings.

3.1 The main program window

The main program window of ESET NOD32 Antivirus is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The following is a description of options within the main menu:

Home – Provides information about the protection status of ESET NOD32 Antivirus.

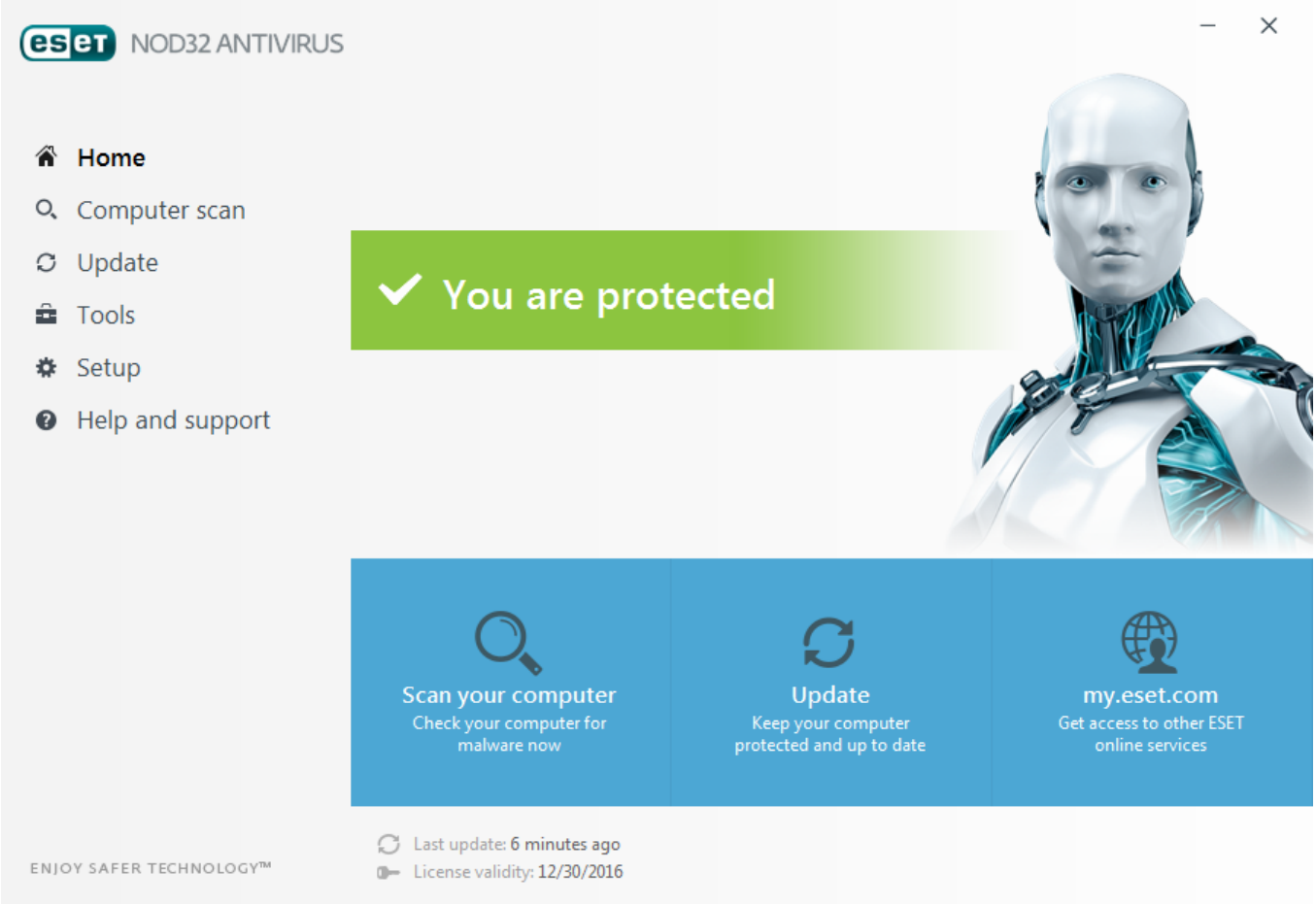
Computer scan – Configure and launch a scan of your computer or create a custom scan.

Update – Displays information about virus signature database updates.

Tools – Provides access to Log files, Protection statistics, Watch activity, Running processes, Scheduler, ESET SysInspector and ESET SysRescue.

Setup – Select this option to adjust the security level for Computer, Internet.

Help and support – Provides access to help files, the ESET Knowledgebase, the ESET website, and links to submit support request.



The **Home** screen contains important information about the current protection level of your computer. The status window displays frequently used features in ESET NOD32 Antivirus. Information about the most recent update and your program's expiration date is also found here.

The green icon and green **Maximum protection** status indicates that maximum protection is ensured.

What to do if the program doesn't work properly?

If an active protection module is working properly its protection status icon will be green. A red exclamation point or orange notification icon indicates that maximum protection is not ensured. Additional information about the protection status of each module, as well as suggested solutions for restoring full protection, will be displayed under **Home**. To change the status of individual modules, click **Setup** and select the desired module.

NOD32 ANTIVIRUS
Home 2
Computer scan
Update
Tools
Setup 4
Help and support
Security alert
Anti-Phishing protection is non-functional
This functionality is not functional because other required program modules are not active.
Antivirus and antispyware protection are paused
This functionality is paused and your computer is not protected against some types of threats.
This is very dangerous and protection should be re-enabled immediately.
Enable Antivirus and antispyware protection
ENJOY SAFER TECHNOLOGY™

The red icon and red **Maximum protection is not ensured** status indicate critical problems.
There are several reasons this status may be displayed, for example:

- **Product not activated** – You can activate ESET NOD32 Antivirus from **Home** by clicking **Activate product** or **Buy now** under **Protection status**.
- **Virus signature database is out of date** – This error will appear after several unsuccessful attempts to update the virus signature database. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.
- **Antivirus and antispyware protection disabled** – You can re-enable antivirus and antispyware protection by clicking **Enable antivirus and antispyware protection**.
- **License expired** – This is indicated by a red protection status icon. The program is not able to update after your license expires. Follow the instructions in the alert window to renew your license.

The orange icon indicates limited protection. For example, there might be a problem updating the program or your license may be nearing its expiration date.
There are several reasons this status may be displayed, for example:

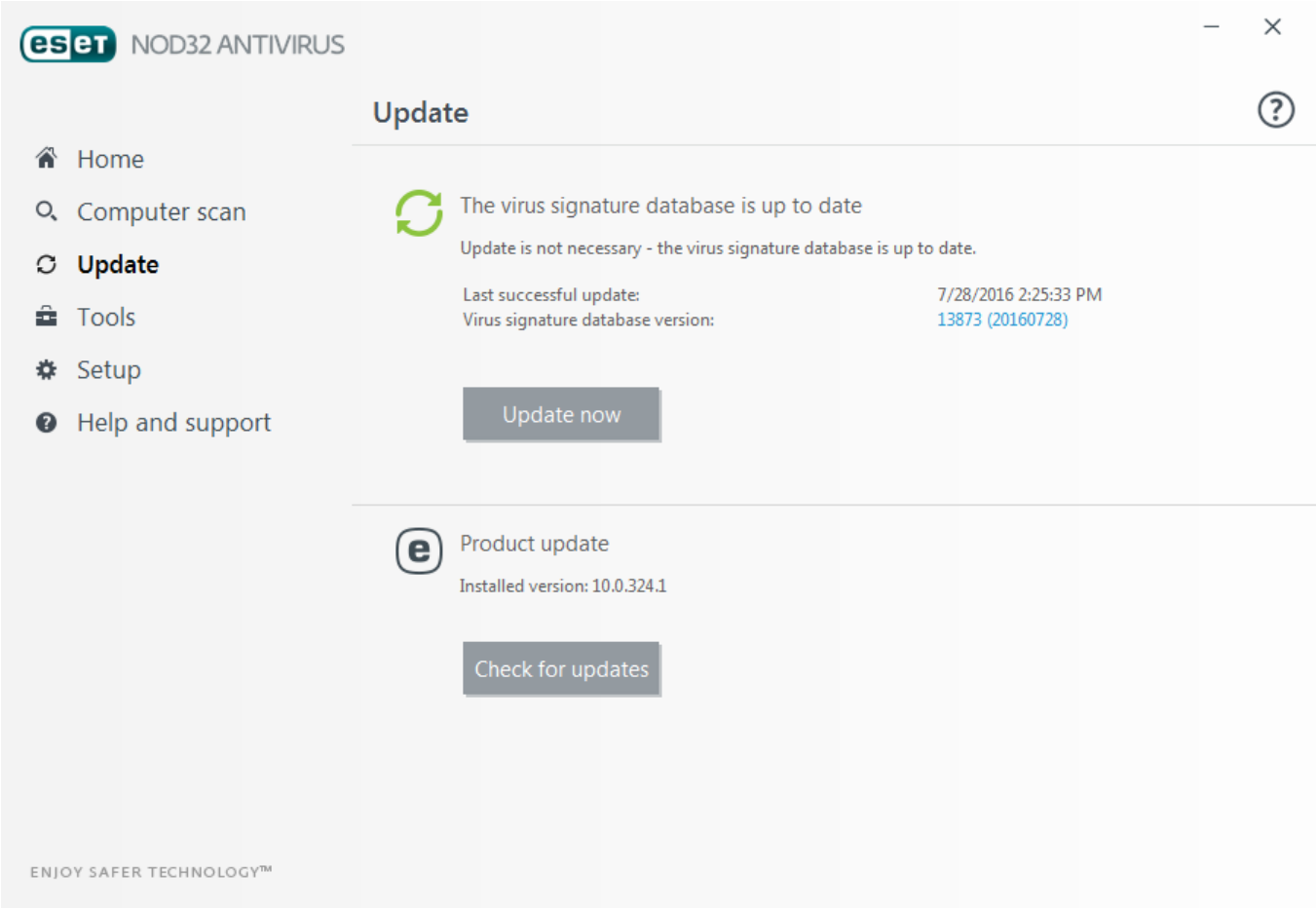
- **Gamer mode active** – Enabling Gamer mode is a potential security risk. Enabling this feature disables all pop-up windows and stops any scheduled tasks.
- **Your license will expire soon** – This is indicated by the protection status icon displaying an exclamation point next to the system clock. After your license expires, the program will not be able to update and the Protection status icon will turn red.

If you are unable to solve a problem using the suggested solutions, click **Help and support** to access help files or search the ESET Knowledgebase. If you still need assistance, you can submit a support request. ESET Customer Care will respond quickly to your questions and help find a resolution.

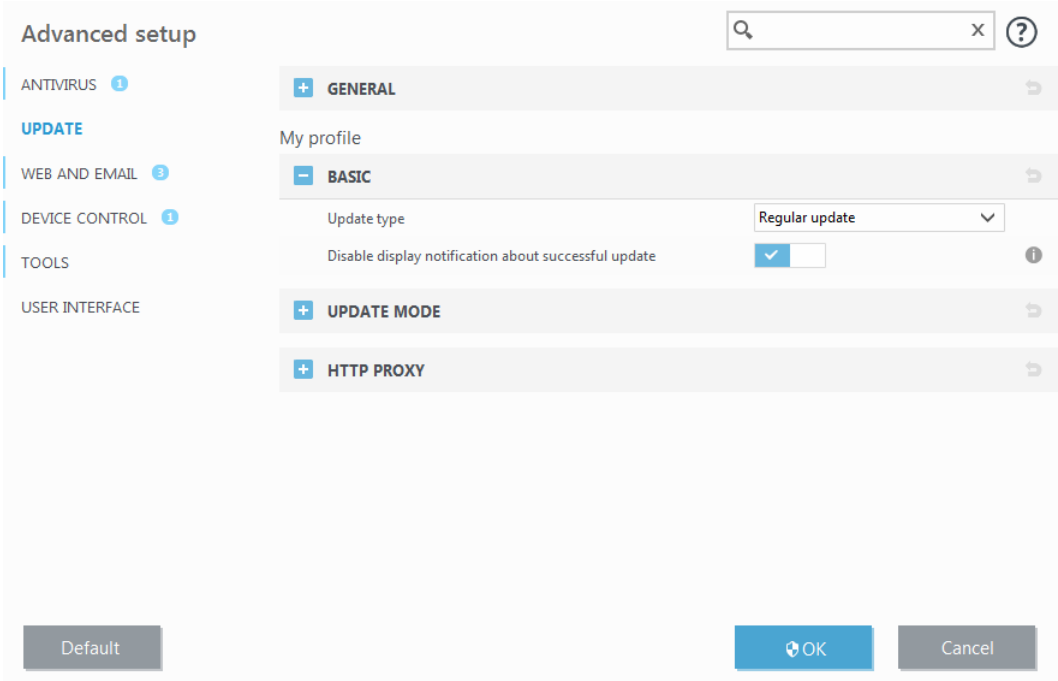
3.2 Updates

Updating the virus signature database and updating program components is an important part of protecting your system against malicious code. Pay careful attention to their configuration and operation. In the main menu, click **Update** and then click **Update now** to check for a virus signature database update.

If the License key was not entered during the activation of ESET NOD32 Antivirus you will be prompted for them at this point.

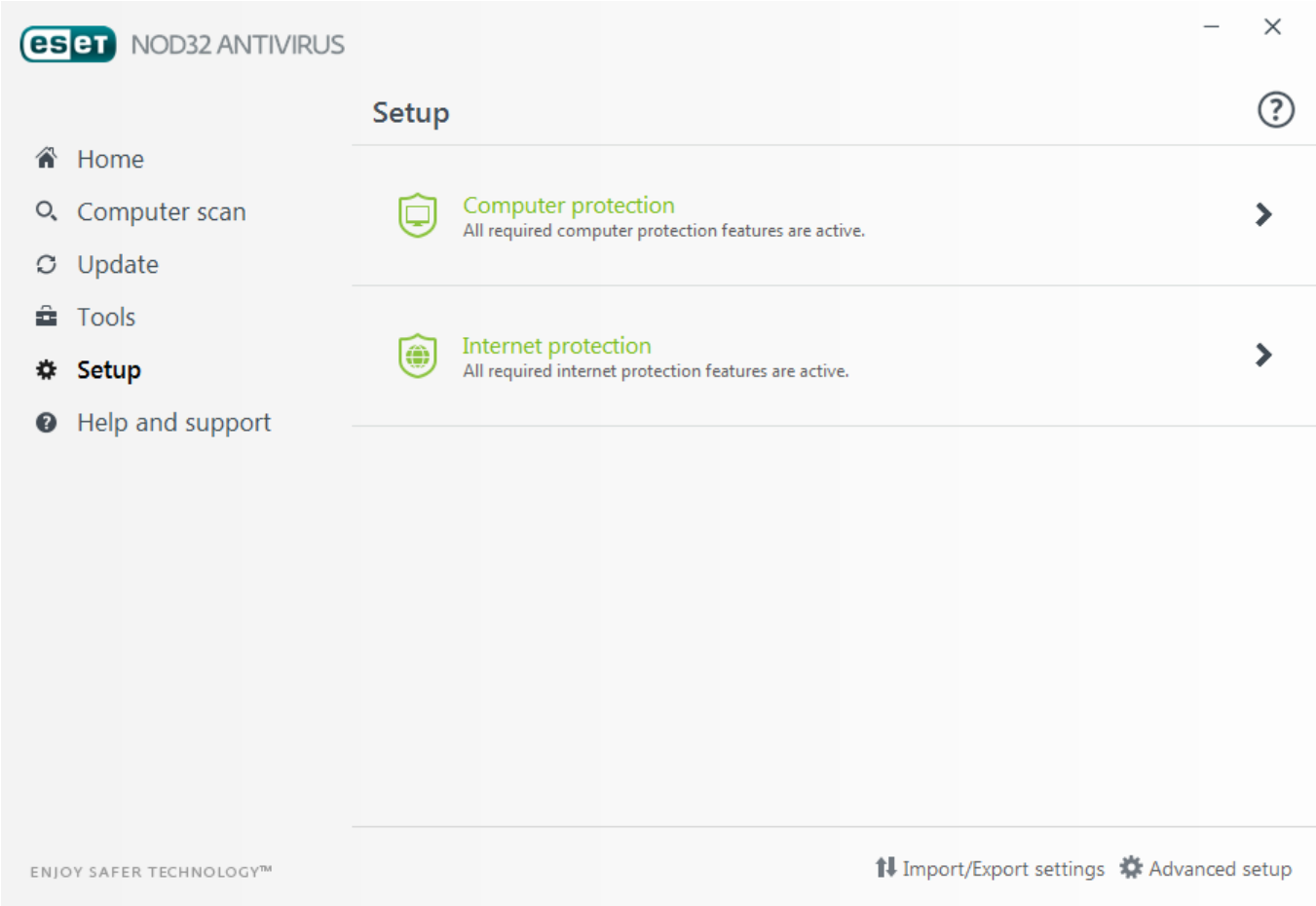


The Advanced setup window (click **Setup** in the main menu and then click **Advanced setup**, or press **F5** on your keyboard) contains additional update options. To configure advanced update options such as update mode, proxy server access and LAN connections, click on particular tab in the **Update** window.



4. Working with ESET NOD32 Antivirus

ESET NOD32 Antivirus setup options allow you to adjust the protection levels of your computer.



The **Setup** menu is divided into the following sections:

Computer protection

Internet protection

Click a component to adjust advanced settings for the corresponding protection module.

Computer protection setup allows you to enable or disable the following components:

- **Real-time file system protection** – All files are scanned for malicious code when they are opened, created, or run on your computer.
- **HIPS** – The HIPS system monitors the events within the operating system and reacts to them according to a customized set of rules.
- **Gamer mode** – Enables or disables Gamer mode. You will receive a warning message (potential security risk) and the main window will turn orange after enabling Gamer mode.

Internet protection setup allows you to enable or disable the following components:

- **Web access protection** – If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** – Monitors communication received through POP3 and IMAP protocol.
- **Anti-Phishing protection** – Filters websites suspected of distributing content intended to manipulate users into submitting confidential information.

To re-enable a disabled security component, click the slider so that it displays a green check mark.

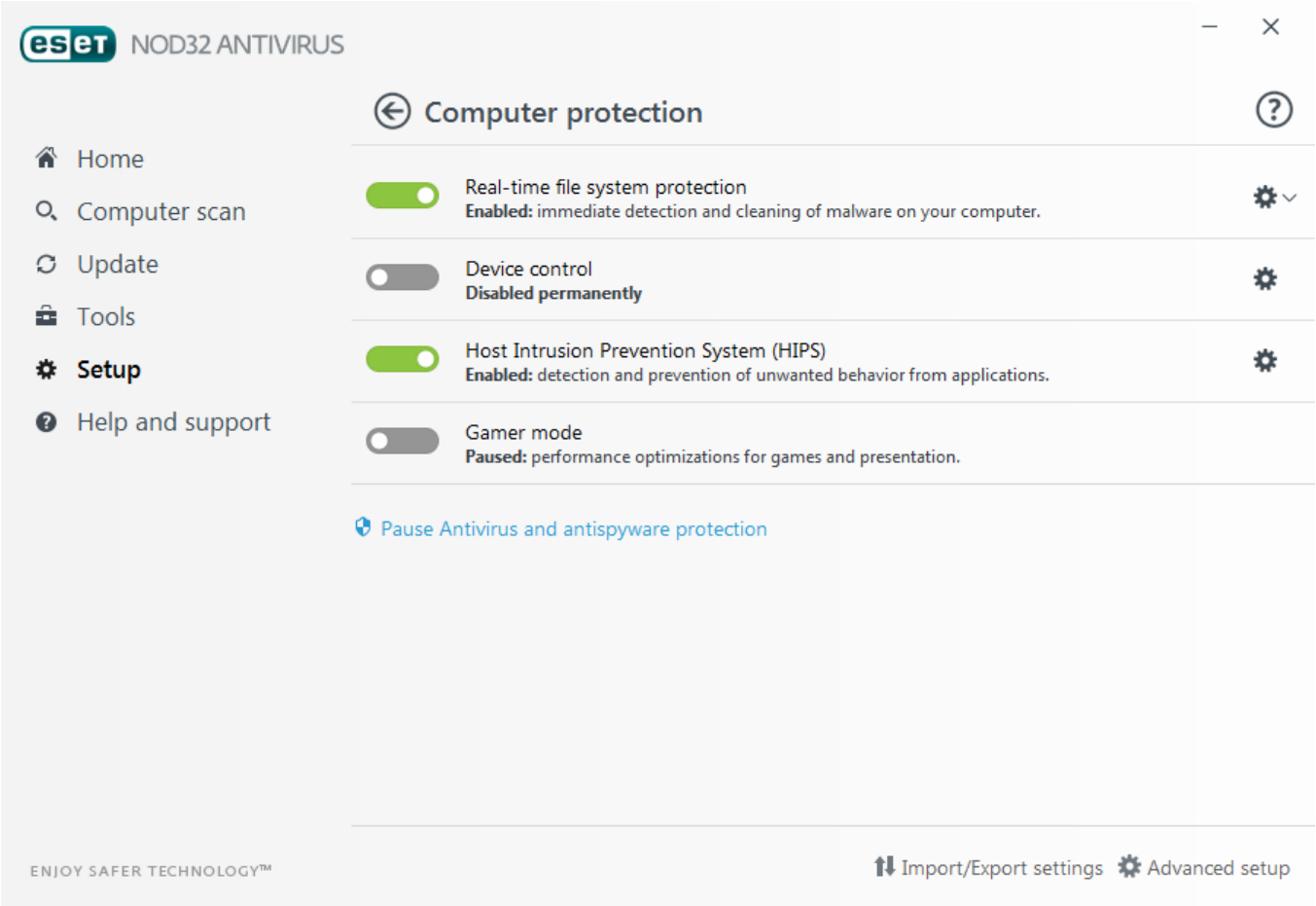
NOTE
When disabling protection using this method, all disabled protection modules will be enabled after a computer restart.

Additional options are available at the bottom of the setup window. Use the **Advanced setup** link to setup more detailed parameters for each module. Use **Import/Export settings** to load setup parameters using an *.xml* configuration file, or to save your current setup parameters to a configuration file.

4.1 Computer protection

Click **Computer Protection** from the **Setup** window to see an overview of all protection modules. To turn off individual modules temporarily, click . Note that this may decrease the protection level of your computer. Click next to a protection module to access advanced settings for that module.

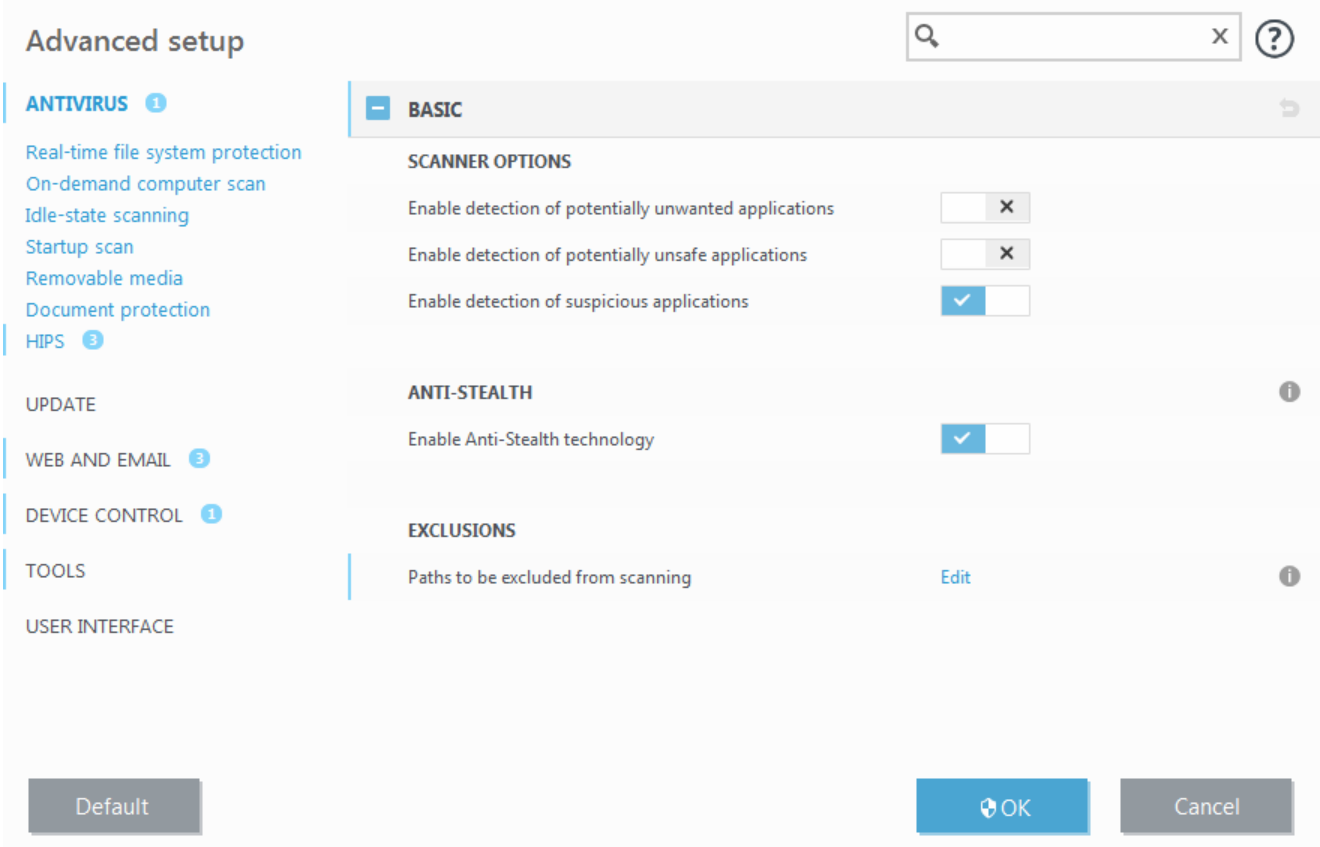
Click > **Edit exclusions** next to **Real-time file system protection** to open the Exclusion setup window, which allows you to exclude files and folders from scanning.



Pause Antivirus and antispyware protection – Disables all antivirus and antispyware protection modules. When you disable protection a window will open where you can determine how long protection is disabled using the **Time interval** drop-down menu. Click **Apply** to confirm.

4.1.1 Antivirus

Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it and then cleaning, deleting or moving it to quarantine.



Scanner options for all protection modules (e.g. Real-time file system protection, Web access protection, ...) allow you to enable or disable detection of the following:

- **Potentially unwanted applications** (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way.
  Read more about these types of applications in the glossary.
- **Potentially unsafe applications** refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default.
  Read more about these types of applications in the glossary.
- **Suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

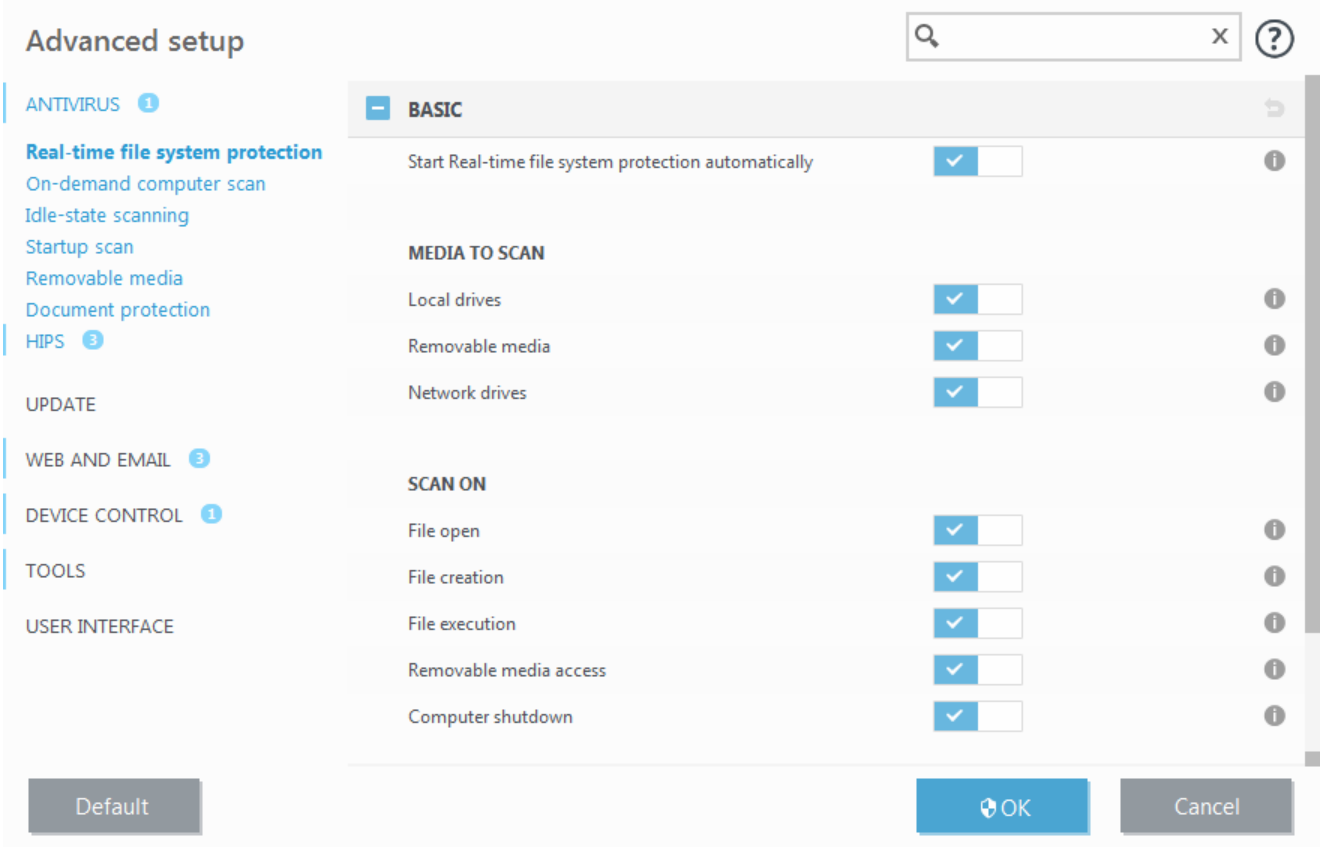
Anti-Stealth technology is a sophisticated system that provides the detection of dangerous programs such as rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan. To exclude an object from scanning see Exclusions.

Enable advanced scanning via AMSI – Microsoft Antimalware Scan Interface tool that allows application developers new malware defenses (Windows 10 only).

4.1.1.1 Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. Real-time file system protection is launched at system startup.



By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging **Start Real-time file system protection automatically** in **Advanced setup** under **Real-time file system protection** > **Basic**.

Media to scan

By default, all types of media are scanned for potential threats:

Local drives – Controls all system hard drives.
Removable media – Controls CD/DVDs, USB storage, Bluetooth devices, etc.
Network drives – Scans all mapped drives.

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

Scan on

By default, all files are scanned upon opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open** – Enables or disables scanning when files are opened.
- **File creation** – Enables or disables scanning when files are created.
- **File execution** – Enables or disables scanning when files are run.
- **Removable media access** – Enables or disables scanning triggered by accessing particular removable media with storage space.
- **Computer shutdown** – Enables or disables scanning triggered by computer shutdown.

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in the ThreatSense engine

parameter setup section), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is controlled using **Smart optimization**. If this **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, press **F5** to open **Advanced setup** and expand **Antivirus** > **Real-time file system protection**. Click **ThreatSense parameter** > **Other** and select or deselect **Enable Smart optimization**.

4.1.1.1.1 Additional ThreatSense parameters

Additional ThreatSense parameters for newly created and modified files

The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. ESET NOD32 Antivirus uses advanced heuristics which can detect new threats before the virus signature database update is released in combination with signature-based scanning methods. In addition to newly-created files, scanning is also performed on **Self-extracting archives** (.sfx) and **Runtime packers** (internally compressed executable files). By default, archives are scanned up to the 10th nesting level, and are checked regardless of their actual size. To modify archive scan settings, deselect **Default archive scan settings**.

Additional ThreatSense parameters for executed files

Advanced heuristics on file execution – By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid® enabled to mitigate impact on system performance.

Advanced heuristics on executing files from removable media – Advanced heuristics emulates code in a virtual environment and evaluates its behavior before the code is allowed to run from removable media.

4.1.1.1.2 Cleaning levels

Real-time protection has three cleaning levels (to access cleaning level settings, click **ThreatSense engine parameter setup** in the **Real-time file system protection** section and then click **Cleaning**).

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

WARNING

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Normal cleaning), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

4.1.1.1.3 When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET NOD32 Antivirus, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click ↩ next to each tab in the window (**Advanced setup** > **Antivirus** > **Real-time file system protection**).

4.1.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file is available for download at http://www.eicar.org/download/eicar.com

4.1.1.1.5 What to do if real-time protection does not work

In this chapter, we describe problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** in the main program window and click **Computer protection** > **Real-time file system protection**.

If real-time protection is not initiated at system startup, it is usually because **Start Real-time file system protection automatically** is disabled. To make sure this option is enabled, navigate to **Advanced setup** (**F5**) and click **Antivirus** > **Real-time file system protection**.

If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two antivirus programs are installed at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system before installing ESET.

Real-time protection does not start

If real-time protection is not initiated at system startup (and **Start Real-time file system protection automatically** is enabled), it may be due to conflicts with other programs. For assistance resolving this issue, please contact ESET Customer Care.

4.1.1.2 Computer scan

The on-demand scanner is an important part of your antivirus solution. It is used to perform scans of files and folders on your computer. From a security standpoint, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular in-depth scans of your system to detect viruses that are not captured by Real-time file system protection when they are written to the disk. This can happen if Real-time file system protection is disabled at the time, the virus database is obsolete or the file is not detected as a virus when it is saved to the disk.

Two types of **Computer scan** are available. **Scan your computer** quickly scans the system without the need to specify scan parameters. **Custom scan** allows you to select from predefined scan profiles designed to target specific locations, and also lets you choose specific scan targets.

Scan your computer

Scan your computer allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Scan your computer is it is easy to operate and does not require detailed scanning configuration. This scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The

cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see Cleaning.

Custom scan

Custom scan lets you specify scanning parameters such as scan targets and scanning methods. The advantage of **Custom scan** is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

Removable media scan

Similar to **Scan your computer** – quickly launch a scan of removable media (such as CD/DVD/USB) that are currently connected to the computer. This may be useful when you connect a USB flash drive to a computer and want to scan its contents for malware and other potential threats.

This type of scan can be also initiated by clicking **Custom scan**, selecting **Removable media** from the **Scan targets** drop-down menu and clicking **Scan**.

Repeat last scan

Allows you to quickly launch the previously performed scan using the same settings it was run with.

See Scan progress for more information about the scanning process.

NOTE
We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**. How do I schedule a weekly computer scan?

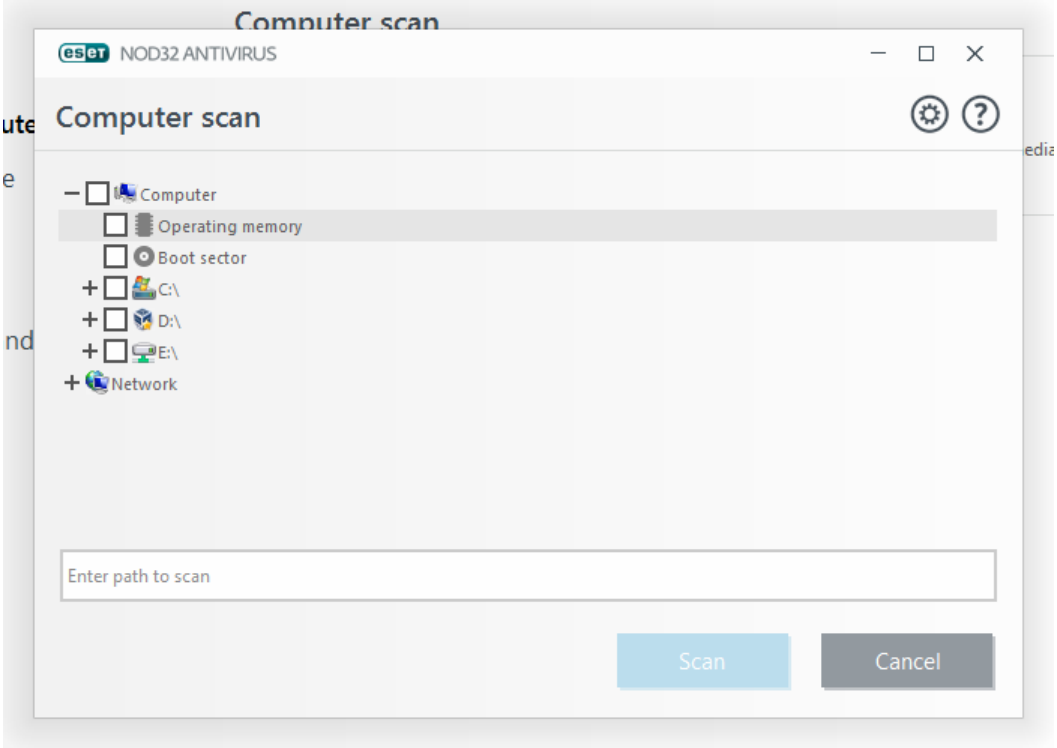
4.1.1.2.1 Custom scan launcher

You can use the Customer Scan to scan specific parts of a disk, rather than the entire disk. To do so, click **Computer scan** > **Custom scan** and select an option from the **Scan targets** drop-down menu, or select specific targets from the folder (tree) structure.

The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets specified by the selected scan profile.
- **Removable media** – Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** – Selects all system hard drives.
- **Network drives** – Selects all mapped network drives.
- **No selection** – Cancels all selections.

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list. This is only possible if no targets are selected in the tree structure and the **Scan targets** menu is set to **No selection**.



You can configure cleaning parameters for the scan under **Advanced setup** > **Antivirus** > **On-demand computer scan** > **ThreatSense parameters** > **Cleaning.** To run a scan with no cleaning action, select **Scan without cleaning**. Scan history is saved to the scan log.

When **Ignore exclusions** is selected, files with extensions that were previously excluded from scanning will be scanned with no exception.

You can choose a profile from the **Scan profile** drop-down menu to be used when scanning specific targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense parameters. Click **Setup...** to set up a customized scan profile. Scan profile options are described under **Other** in ThreatSense parameters.

Click **Scan** to execute the scan using the custom parameters that you have set.

Scan as Administrator allows you to execute the scan under the Administrator account. Use this if the current user doesn't have privileges to access the files you want to scan. This button is not available if the current user cannot call UAC operations as Administrator.

NOTE
You can view the computer scan log when a scan completes by clicking **Show log**.

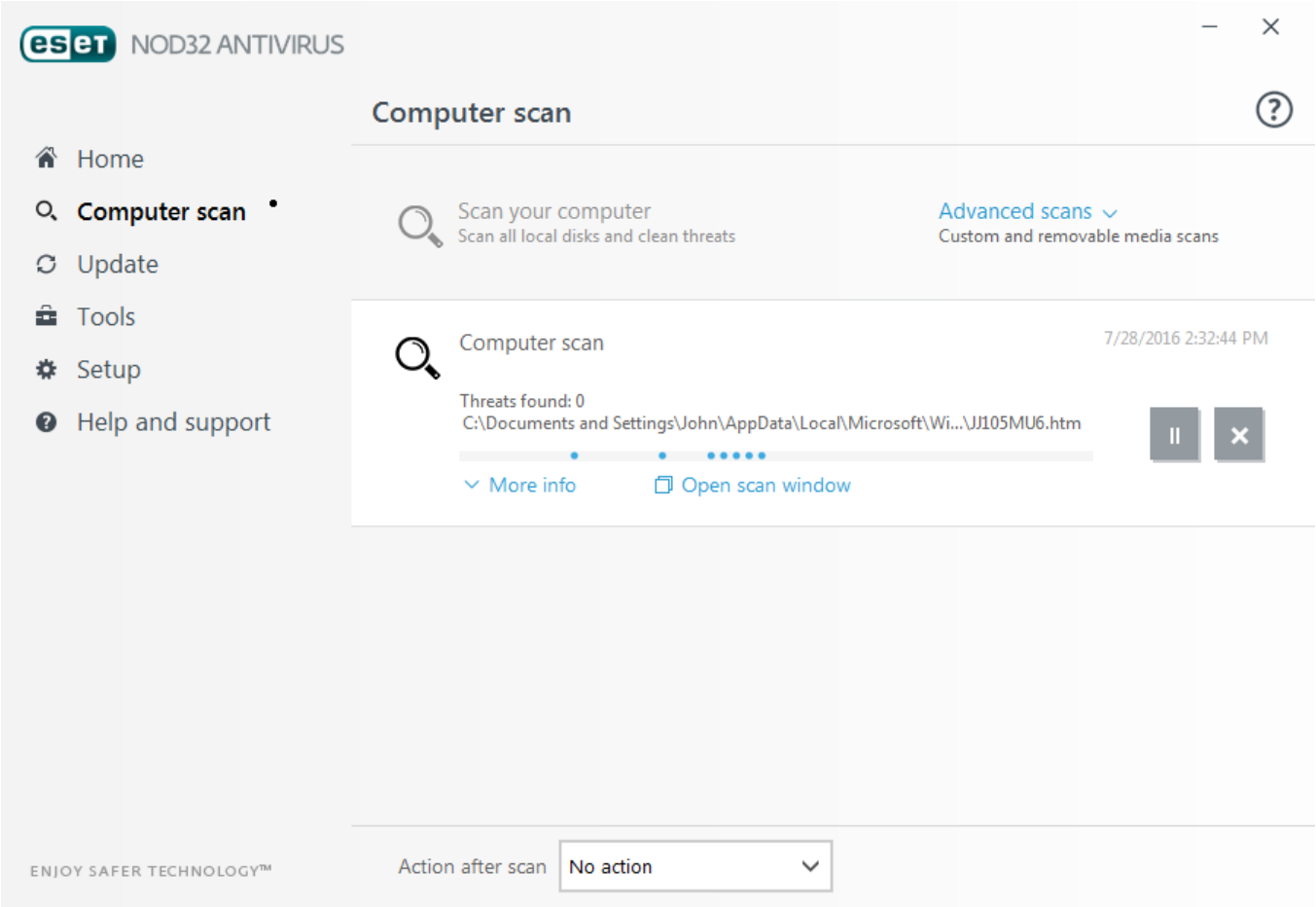
4.1.1.2.2 Scan progress

The scan progress window shows the current status of the scan and information about the number of files found that contain malicious code.

NOTE
It is normal that some files, such as password protected files or files being exclusively used by the system (typically *pagefile.sys* and certain log files), cannot be scanned.

Scan progress – The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.
Target – The name of the currently scanned object and its location.
Threats found – Shows the total number of scanned files, threats found and threats cleaned during a scan.
Pause – Pauses a scan.
Resume – This option is visible when scan progress is paused. Click **Resume** to continue scanning.
Stop – Terminates the scan.
Scroll scan log – If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.

NOTE
Click the magnifier or arrow to show details about the scan that is currently running. You can run another parallel scan by clicking **Scan your computer** or **Custom scan**.



Action after scan – Triggers a scheduled shutdown or reboot when the computer scan finishes. Once the scan has finished, a shutdown confirmation dialog window will open with a 60 second timeout.

4.1.1.2.3 Scan profiles

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced setup window (F5) and click **Antivirus** > **On-demand computer scan** > **Basic** > **List of profiles**. The **Profile manager** window includes the **Selected profile** drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

NOTE
Suppose that you want to create your own scan profile and the **Scan your computer** configuration is partially suitable, but you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. Enter the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements and click **OK** to save your new profile.

4.1.1.2.4 Computer scan log

The computer scan log gives you general information about the scan such as:

- Time of completion
- Total scanning time
- Number of threats found
- Number of scanned objects
- Scanned disk, folders and files
- Date and time of scan
- Version of virus signature database

4.1.1.3 Idle-state scanning

Click the switch next to **Enable Idle-state scanning** under **Advanced setup** > **Antivirus** > **Idle-state scanning** > **Basic** to allow automatic system scans when your computer is not in use.

By default, the idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting with the **Run even if computer is powered from battery** feature.

Turn on **Enable logging** to record a computer scan output in the Log files section (from the main program window click **Tools** > **Log files** and then select **Computer scan** from the **Log** drop-down menu).

Idle-state detection will run when your computer is in the following states:

- Screen saver
- Computer lock
- User log off

Click ThreatSense parameters to modify scan parameters (for example, detection methods) for the Idle-state scanner.

4.1.1.4 Startup scan

By default the automatic startup file check will be performed on system startup and during virus signature database updates. This scan is dependent upon the Scheduler configuration and tasks.

The startup scan options is part of a **System startup file check** scheduler task. To modify its settings, navigate to **Tools** > **Scheduler**, click on **Automatic startup file check** and then **Edit**. In the last step, the Automatic startup file check window will appear (see the following chapter for more details).

For detailed instructions about Scheduler task creation and management, see Creating new tasks.

4.1.1.4.1 Automatic startup file check

When creating a System startup file check scheduled task, you have several options to adjust the following parameters:

The **Commonly used files** drop-down menu specifies the scan depth for files run at system startup based on secret sophisticated algorithm. Files are arranged in descending order according to the following criteria:

- **All registered files** (most files scanned)
- **Rarely used files**
- **Commonly used files**
- **Frequently used files**
- **Only the most frequently used files** (least files scanned)

Two specific groups are also included:

- **Files run before user logon** – Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll's, etc.).
- **Files run after user logon** - Contains files from locations that may only be accessed after a user has logged in (includes files that are only run by a specific user, typically files in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Lists of files to be scanned are fixed for each aforementioned group.

Scan priority – The level of priority used to determine when a scan will start:

- **When idle** – the task will be performed only when the system is idle,
- **Lowest** – when the system load is the lowest possible,
- **Lower** – at a low system load,
- **Normal** – at an average system load.

4.1.1.5 Exclusions

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. However, there are situations where you may need to exclude an object, for example large database entries that would slow your computer during a scan or software that conflicts with the scan.

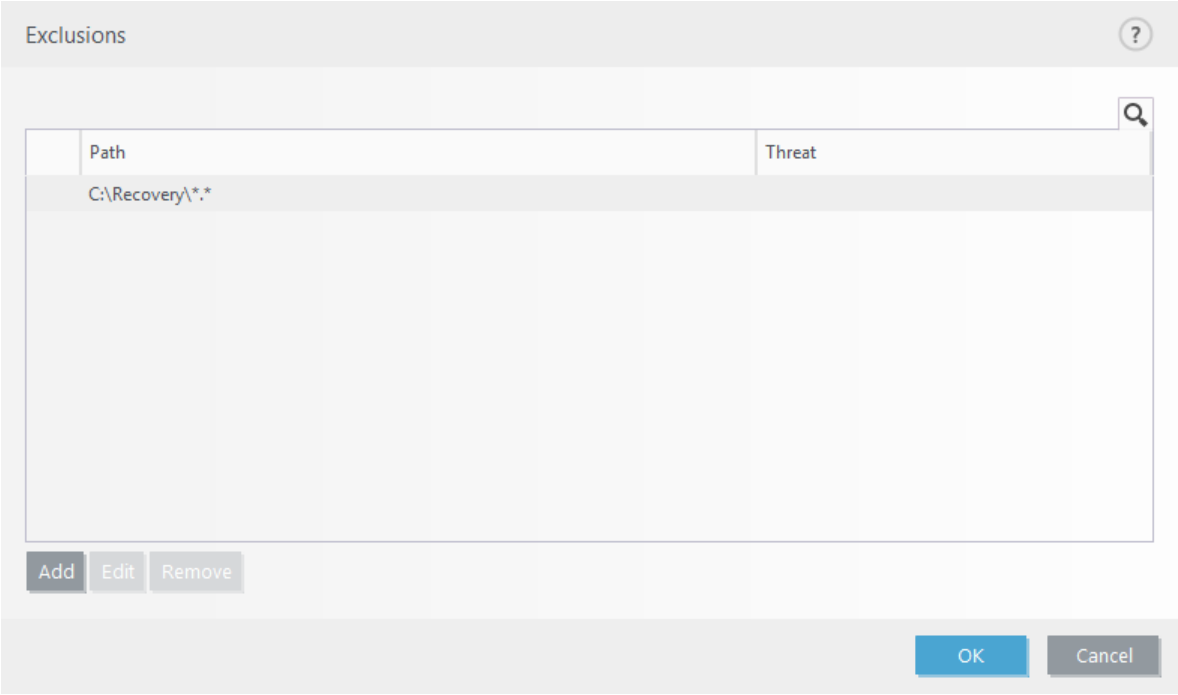
To exclude an object from scanning:

1. Click **Add**,
2. Enter the path to an object or select it in the tree structure.

You can use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters.

Examples

- If you wish to exclude all files in a folder, type the path to the folder and use the mask “*.*”.
- To exclude an entire drive including all files and subfolders, use the mask "D:*".
- If you want to exclude doc files only, use the mask “*.doc“.
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D????.exe”. Question marks replace the missing (unknown) characters.



NOTE
A threat within a file will not be detected by the Real-time file system protection module or Computer scan module if a file meets the criteria for exclusion from scanning.

Columns

Path – Path to excluded files and folders.

Threat – If there is a name of a threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations and it can be created either in the threat alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or by clicking **Tools** > **Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from detection** from the context menu.

Control elements

Add – Excludes objects from detection.

Edit – Enables you to edit selected entries.

Remove – Removes selected entries.

4.1.1.6 ThreatSense parameters

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense parameters** in the Advanced setup window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors – Scans boot sectors for the presence of viruses in the master boot record.

Email files – The program supports the following extensions: DBX (Outlook Express) and EML.

Archives – The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives – Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers – After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics – A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not covered by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures – Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

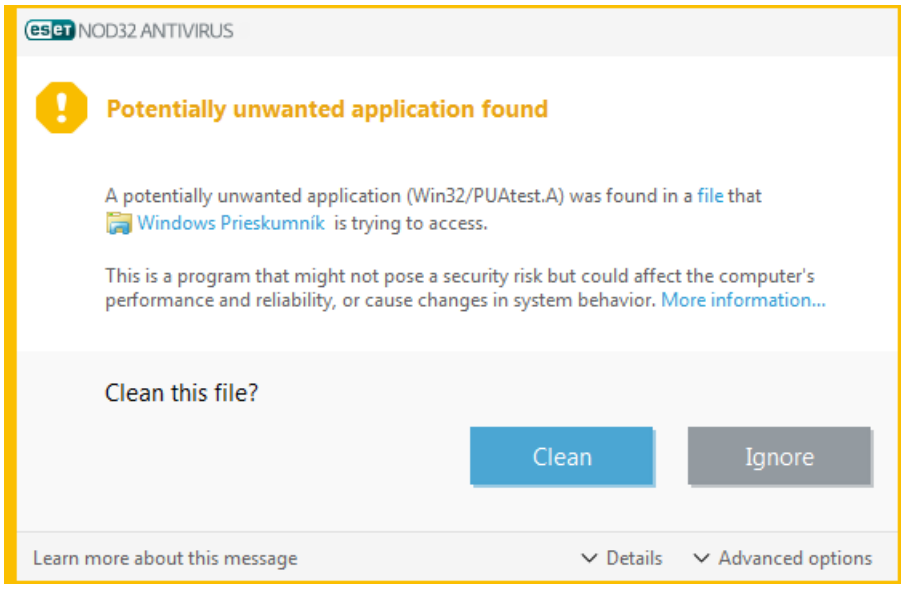
A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives. There are some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software, such as trojan horses or worms.

Warning - Potential threat found

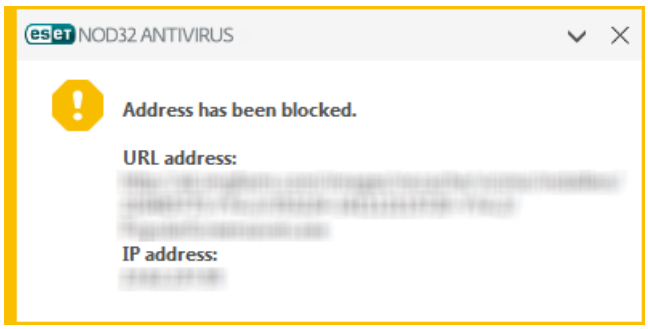
When a potentially unwanted application is detected, you can decide which action to take:

1. **Clean/Disconnect**: This option ends the action and prevents the potential threat from entering your system.
2. **Ignore**: This option allows a potential threat to enter your system.
3. To allow the application to run on your computer in the future without interruption, click **Advanced options** and

then select the check box next to **Exclude from detection**.

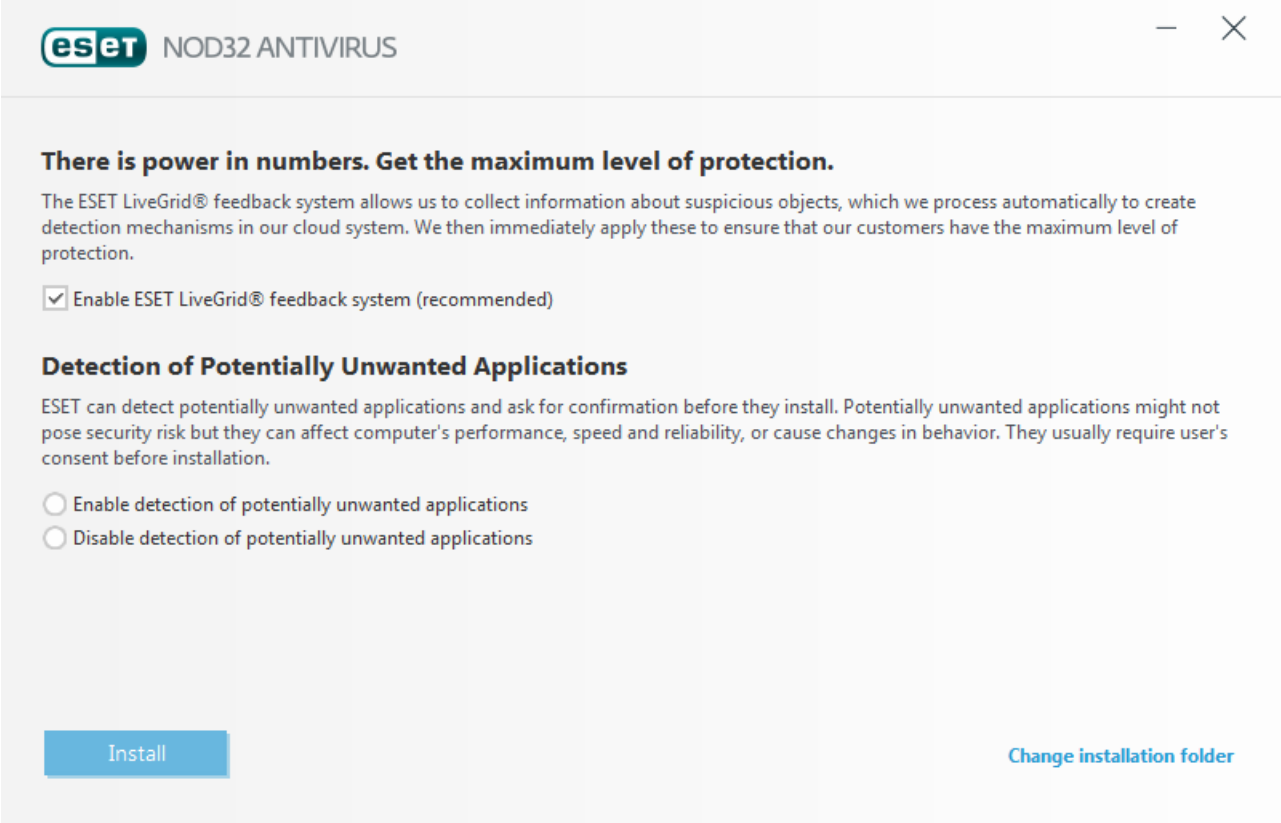

NOD32 ANTIVIRUS
Potentially unwanted application found
A potentially unwanted application (Win32/PUAtest.A) was found in a file that
Windows Prieskumník is trying to access.
This is a program that might not pose a security risk but could affect the computer's performance and reliability, or cause changes in system behavior. More information...
Clean this file?
Clean
Ignore
Learn more about this message
Details
Advanced options

When a potentially unwanted application is detected and cannot be cleaned, an **Address has been blocked** notification will be displayed. For more information about this event navigate to **Tools** > **Log files** > **Filtered websites** from the main menu.



Potentially unwanted applications - Settings

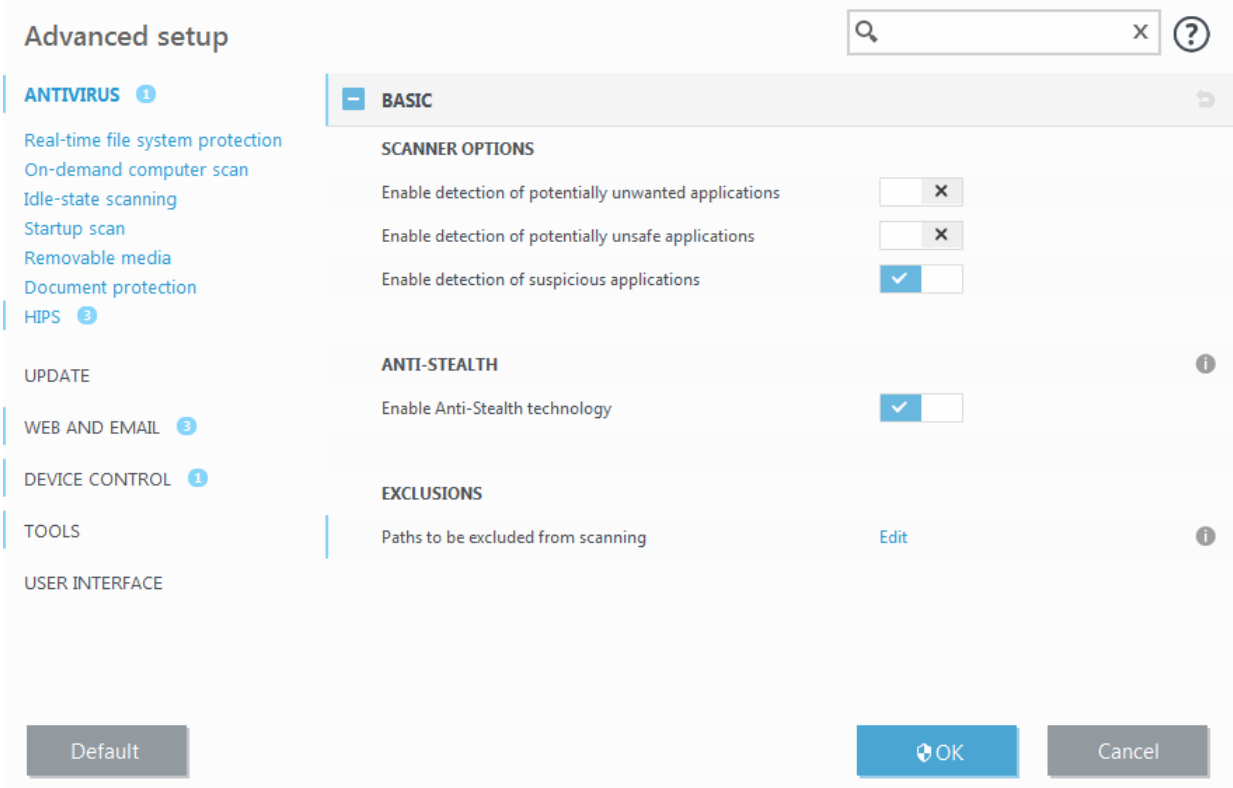
While installing your ESET product, you can decide whether to enable detection of potentially unwanted applications, as shown below:


NOD32 ANTIVIRUS
There is power in numbers. Get the maximum level of protection.
The ESET LiveGrid® feedback system allows us to collect information about suspicious objects, which we process automatically to create detection mechanisms in our cloud system. We then immediately apply these to ensure that our customers have the maximum level of protection.
Enable ESET LiveGrid® feedback system (recommended)
Detection of Potentially Unwanted Applications
ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications
Install
Change installation folder

WARNING
Potentially unwanted applications may install adware, toolbars, or contain other unwanted and unsafe program features.

These settings can be modified in your program settings at any time. To enable or disable the detection of Potentially unwanted, unsafe or suspicious applications, follow these instructions:

1. Open your ESET product. How do I open my ESET product?
2. Press the **F5** key to access **Advanced setup**.
3. Click **Antivirus** and enable or disable options **Enable detection of potentially unwanted applications**, **Enable detection of potentially unsafe applications** and **Enable detection of suspicious applications** according to your preferences. Confirm by clicking **OK**.



Potentially unwanted applications - Software wrappers

A software wrapper is a special type of application modification that is used by some file-hosting websites. It is a third-party tool that installs the program you intended to download but adds additional software, such as toolbars or adware. The additional software may also make changes to your web browser's home page and search settings. Also, file-hosting websites often do not notify the software vendor or download recipient that modifications have been made, and often hide options to opt out. For these reasons, ESET classifies software wrappers as a type of potentially unwanted application to allow users to accept the download or not.

Please see this ESET Knowledgebase article for an updated version of this help page.

Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate programs such as remote access tools, password-cracking applications and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS) – Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.

Enable Smart optimization – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

Preserve last access timestamp – Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

Maximum scan time for object (sec.) – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive scan setup

Archive nesting level – Specifies the maximum depth of archive scanning. Default value: *10*.

Maximum size of file in archive – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

NOTE
We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

4.1.1.6.1 Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning.

4.1.1.6.2 File extensions excluded from scanning

An extension is a part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning.

Excluding files is sometimes necessary if scanning certain file types prevents the program that is using certain extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

Using the **Add** and **Remove** buttons, you can allow or prohibit the scanning of specific file extensions. To add a new extension to the list, click **Add** type the extension into the blank field and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons. When multiple selection is enabled, extensions will be shown in the list. Select an extension in the list and click **Remove** to delete that extension from the list. If you want to edit a selected extension click **Edit**.

The special symbol ? (question mark) can be used. The question mark represents any symbol.

NOTE
In order to see the exact extension (if any) of a file in a Windows operating system you have to uncheck the **Hide extensions for known file types** option at **Control Panel** > **Folder Options** > **View** (tab) and apply this change.

4.1.1.7 An infiltration is detected

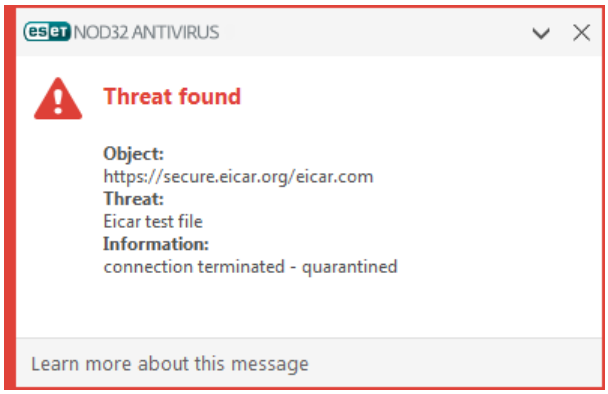
Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, diskettes, etc.).

Standard behavior

As a general example of how infiltrations are handled by ESET NOD32 Antivirus, infiltrations can be detected using:

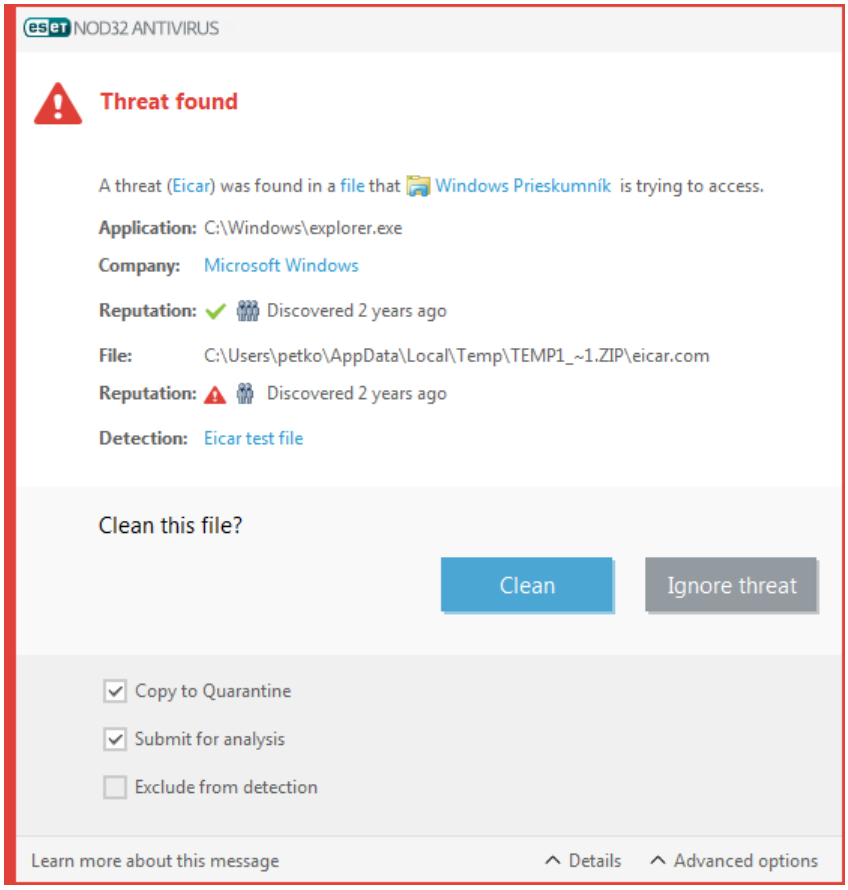
- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

Each uses the standard cleaning level and will attempt to clean the file and move it to Quarantine or terminate the connection. A notification window is displayed in the notification area at the bottom right corner of the screen. For more information about cleaning levels and behavior, see Cleaning.



Cleaning and deleting

If there is no predefined action to take for Real-time file system protection, you will be prompted to select an option in the alert window. Usually the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, as this will leave infected files uncleaned. The exception to this is when you are sure that a file is harmless and has been detected by mistake.



Apply cleaning if a file has been attacked by a virus that has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

If an infected file is “locked“ or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Multiple threats

If any infected files were not cleaned during Computer scan (or the Cleaning level was set to **No Cleaning**), an alert window prompting you to select actions for those files is displayed. Select actions for the files (actions are set individually for each file in the list) and then click **Finish**.

Deleting files in archives

In Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a Strict cleaning scan, with Strict cleaning enabled an archive will be deleted if it contains at least one infected file regardless of the status of other files in the archive.

If your computer is showing signs of a malware infection, e.g., it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET NOD32 Antivirus and click Computer scan
- Click **Scan your computer** (for more information, see Computer scan)
- After the scan has finished, review the log for the number of scanned, infected and cleaned files

If you only want to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

4.1.1.8 Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that do not handle a high number of Microsoft Office documents.

To activate Document protection, open the **Advanced setup** window (press **F5**) > **Antivirus** > **Document protection** and click the **Integrate into system** switch.

NOTE
This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

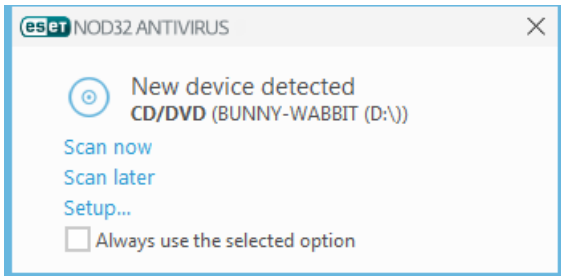
4.1.2 Removable media

ESET NOD32 Antivirus provides automatic removable media (CD/DVD/USB/...) scanning. This module allows you to scan an inserted media. This may be useful if the computer administrator wishes to prevent the users from using removable media with unsolicited content.

Action to take after inserting removable media - Select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). If **Show scan options** is selected, a notification will display which allows you to choose a desired action:

- **Do not scan** – No action will be performed and the **New device detected** window will be closed.
- **Automatic device scan** – An on-demand computer scan of the inserted removable media device will be performed.
- **Show scan options** – Opens the Removable media setup section.

When a removable media is inserted, following dialog will shown:



Scan now – This will trigger scan of removable media.

Scan later – Scan of removable media will be postponed.

Setup – Opens the Advanced setup.

Always use the selected option – When selected, same action will be performed when a removable media is inserted another time.

In addition, ESET NOD32 Antivirus features the Device control functionality, which allows you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

4.1.3 Device control

Device control

ESET NOD32 Antivirus provides automatic device (CD/DVD/USB/...) control. This module allows you to scan, block or adjust extended filters/permissions and define a users ability to access and work with a given device. This may be useful if the computer administrator wishes to prevent use of devices with unsolicited content by users.

Supported external devices:

- Disk Storage (HDD, USB removable disk)
- CD/DVD
- USB Printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device
- Microphone
- All device types

Device control setup options can be modified in **Advanced setup** (F5) > **Device control**.

Turning the switch on next to **Integrate into system** activates the Device control feature in ESET NOD32 Antivirus; you will need to restart your computer for this change to take effect. Once Device control is enabled, the **Rules** will become active, allowing you to open the Rules editor window.

NOTE
You can create different groups of devices for which different rules will be applied. You can also create only one group of devices for which the rule with action **Read/Write** or **Read only** will be applied. This ensures blocking unrecognized devices by Device control when connected to your computer.

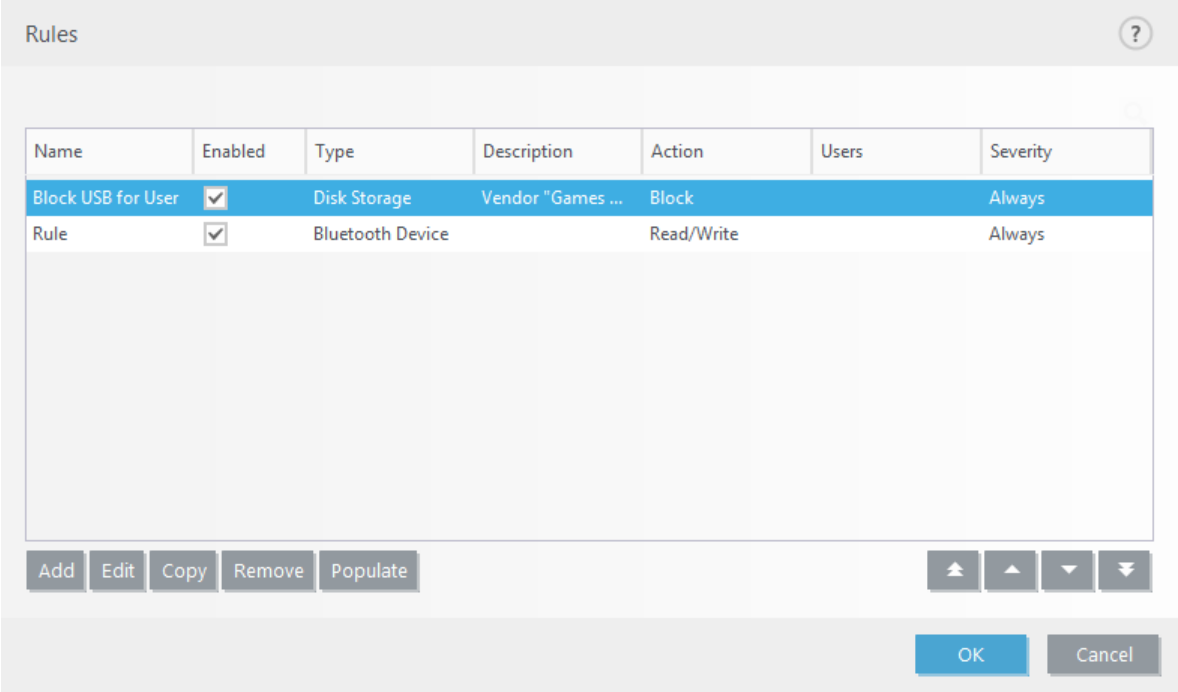
If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device will not be granted.

Webcam Protection

Turning the switch on next to **Integrate into system** activates the Webcam Protection feature in ESET NOD32 Antivirus. Once Webcam Protection is enabled, the **Rules** will become active, allowing you to open the Rules editor window.

4.1.3.1 Device control rules editor

The **Device control rules editor** window displays existing rules and allows for precise control of external devices that users connect to the computer.



Particular devices can be allowed or blocked per user or user group and based on additional device parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, type of external device, action to perform after connecting an external device to your computer and log severity.

Click **Add** or **Edit** to manage a rule. Click **Copy** to create a new rule with predefined options used for another selected rule. XML strings displayed when clicking a rule can be copied to the clipboard to help system administrators to export/import these data and use them, for example in ESET Remote Administrator.

By pressing CTRL and clicking, you can select multiple rules and apply actions, such as deleting or moving them up or down the list, to all selected rules. The **Enabled** check box disables or enables a rule; this can be useful if you don't wish to delete a rule permanently in case you wish to use it in the future.

The control is accomplished by rules that are sorted in the order determining their priority, with higher priority rules on top.

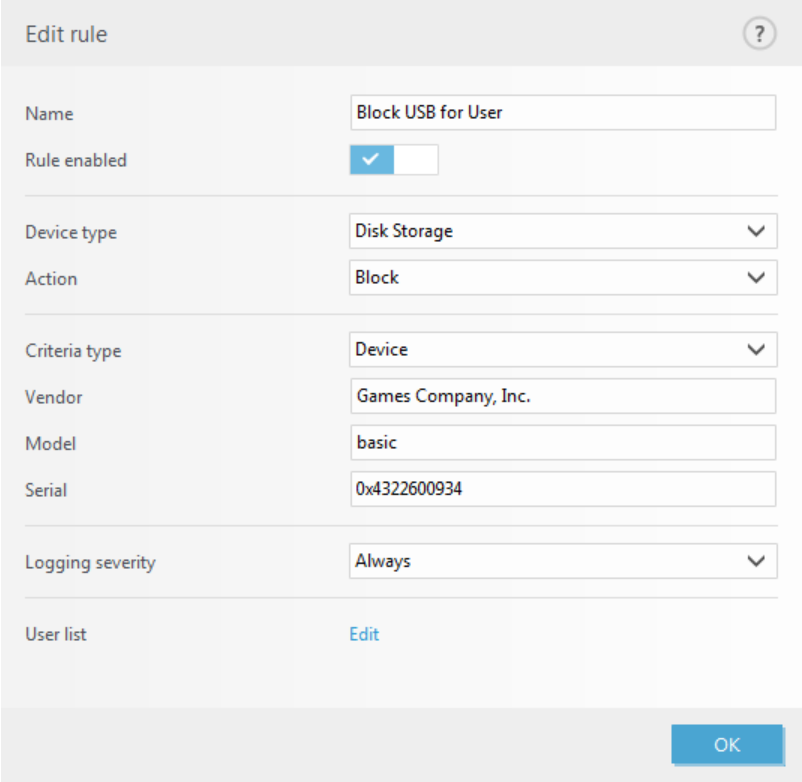
Log entries can be viewed from the main window of ESET NOD32 Antivirus in **Tools** > **Log files**.

The Device control log records all occurrences where Device control is triggered.

Click **Populate** to auto-populate removable media device parameters for devices connected to your computer.

4.1.3.2 Adding Device control rules

A Device control rule defines the action that will be taken when a device meeting the rule criteria is connected to the computer.



Enter a description of the rule into the **Name** field for better identification. Click the switch next to **Rule enabled** to disable or enable this rule; this can be useful if you don't want to delete the rule permanently.

Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). Device type information is collected from the operating system and can be seen in the system Device manager if a device is connected to the computer. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Smart card readers include all readers of smart cards with an embedded integrated circuit, such as SIM cards or authentication cards. Examples of imaging devices are scanners or cameras. Because these devices only provide information about their actions and do not provide information about users, they can only be blocked globally.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices allow you to select one of the following rights settings:

- **Read/Write** – Full access to the device will be allowed.
- **Block** – Access to the device will be blocked.
- **Read Only** – Only read access to the device will be allowed.
- **Warn** – Each time that a device is connected, the user will be notified if it is allowed/blocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed upon subsequent connections of the same device.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example **Read Only** is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).

Criteria type – Select **Device group** or **Device.**

Additional parameters shown below can be used to fine-tune rules and tailor them to devices. All parameters are case-insensitive:

- **Vendor** – Filter by vendor name or ID.
- **Model** – The given name of the device.
- **Serial** – External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

NOTE
If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

NOTE
To view information about a device, create a rule for that type of device, connect the device to your computer and then check the device details in the Device control log.

Logging severity

ESET NOD32 Antivirus saves all important events in a log file, which can be viewed directly from the main menu. Click **Tools** > **Log files** and then select **Device control** from the **Log** drop-down menu.

- **Always** – Logs all events.
- **Diagnostic** – Logs information needed to fine-tune the program.
- **Information** – Records informative messages, including successful update messages, plus all records above.
- **Warning** – Records critical errors and warning messages.
- **None** – No logs will be recorded.

Rules can be limited to certain users or user groups by adding them to the **User list**:

- **Add** – Opens the **Object types: Users or Groups** dialog window that allows you to select desired users.
- **Remove** – Removes the selected user from the filter.

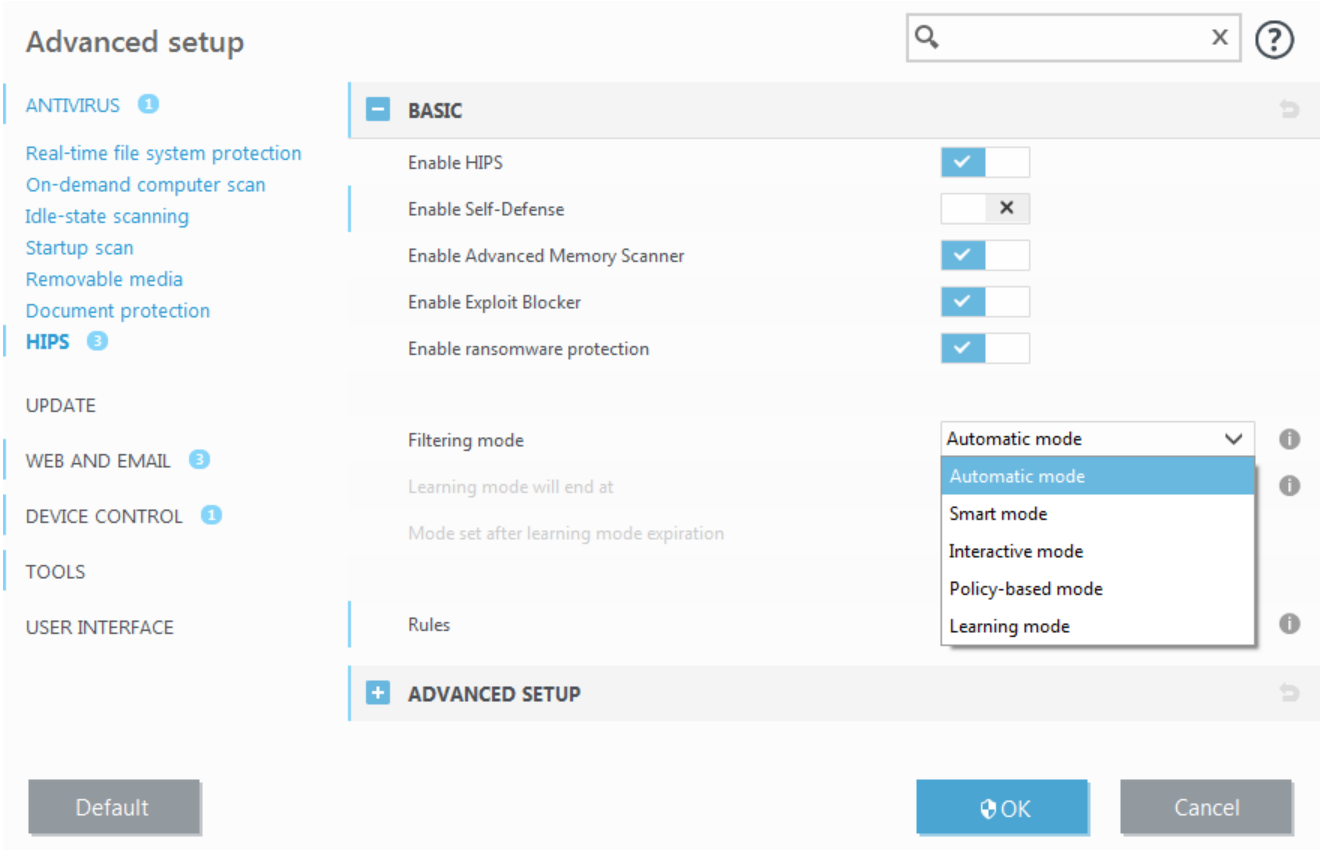
NOTE
All devices can be filtered by user rules, (for example imaging devices do not provide information about users, only about actions).

4.1.4 Host-based Intrusion Prevention System (HIPS)

WARNING
Changes to HIPS settings should only be made by an experienced user. Incorrect configuration of HIPS settings can lead to system instability.

The **Host-based Intrusion Prevention System (HIPS)** protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

HIPS settings can be found under **Advanced setup** (F5) > **Antivirus** > **HIPS** > **Basic**. The HIPS state (enabled/disabled) is shown in the ESET NOD32 Antivirus main program window, under **Setup** > **Computer protection**.



ESET NOD32 Antivirus uses built-in **Self-Defense** technology to prevent malicious software from corrupting or disabling your antivirus and antispyware protection, so you can be sure your system is protected at all times. It is necessary to restart Windows to disable HIPS or Self-Defense.

Enable Protected Service – Enables kernel protection (Windows 8.1, 10).

Advanced memory scanner works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.

Exploit Blocker is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.

Ransomware protection is another layer of protection that works as a part of HIPS feature. You must have the LiveGrid reputation system enabled for Ransomware protection to work. Read more about this type of protection here.

Filtering can be performed in one of four modes:

Automatic mode – Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.

Smart mode – The user will only be notified about very suspicious events.

Interactive mode – User will be prompted to confirm operations.

Policy-based mode – Operations are blocked.

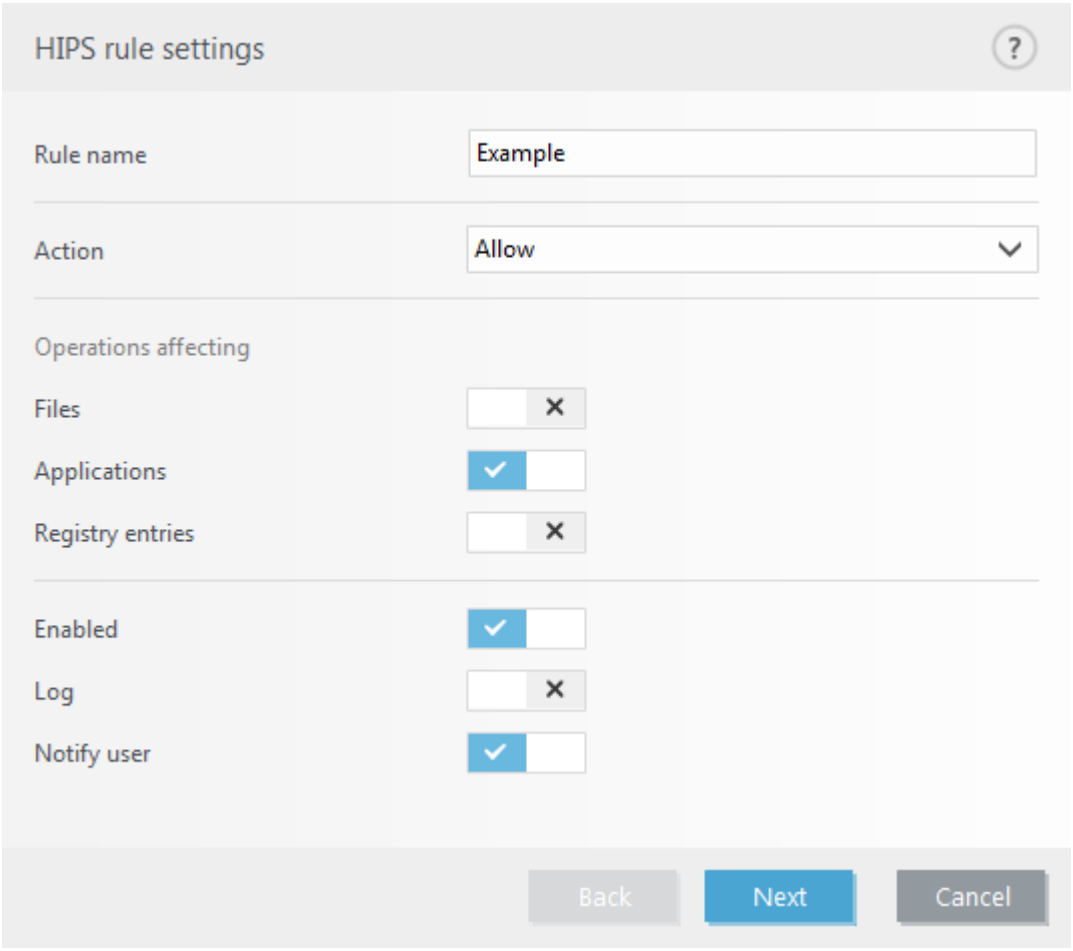
Learning mode – Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in the automatic mode. When you select Learning mode from the HIPS Filtering mode drop down menu, the **Learning mode will end at** setting will become available. Select the time span that you want to engage learning mode for, the maximum duration is 14 days. When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

Mode set after learning mode expiration – Select the filtering mode after learning mode expires.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to those used by the personal firewall. Click **Edit** to open the HIPS rule management window. Here you can select, create, edit or delete rules.

In the following example, we will demonstrate how to restrict unwanted behavior of applications:

1. Name the rule and select **Block** from the **Action** drop-down menu.
2. Enable the **Notify user** switch to display a notification any time that a rule is applied.
3. Select at least one operation for which the rule will be applied. In the **Source applications** window, select **All applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.
4. Select **Modify state of another application** (all operations are described in product help, which can be accessed by pressing F1).
5. Select **Specific applications** from the drop-down menu and **Add** one or several applications you want to protect.
6. Click **Finish** to save your new rule.



4.1.4.1 Advanced setup

The following options are useful for debugging and analyzing an application's behavior:

Drivers always allowed to load – Selected drivers are always allowed to load regardless of configured filtering mode, unless explicitly blocked by user rule.

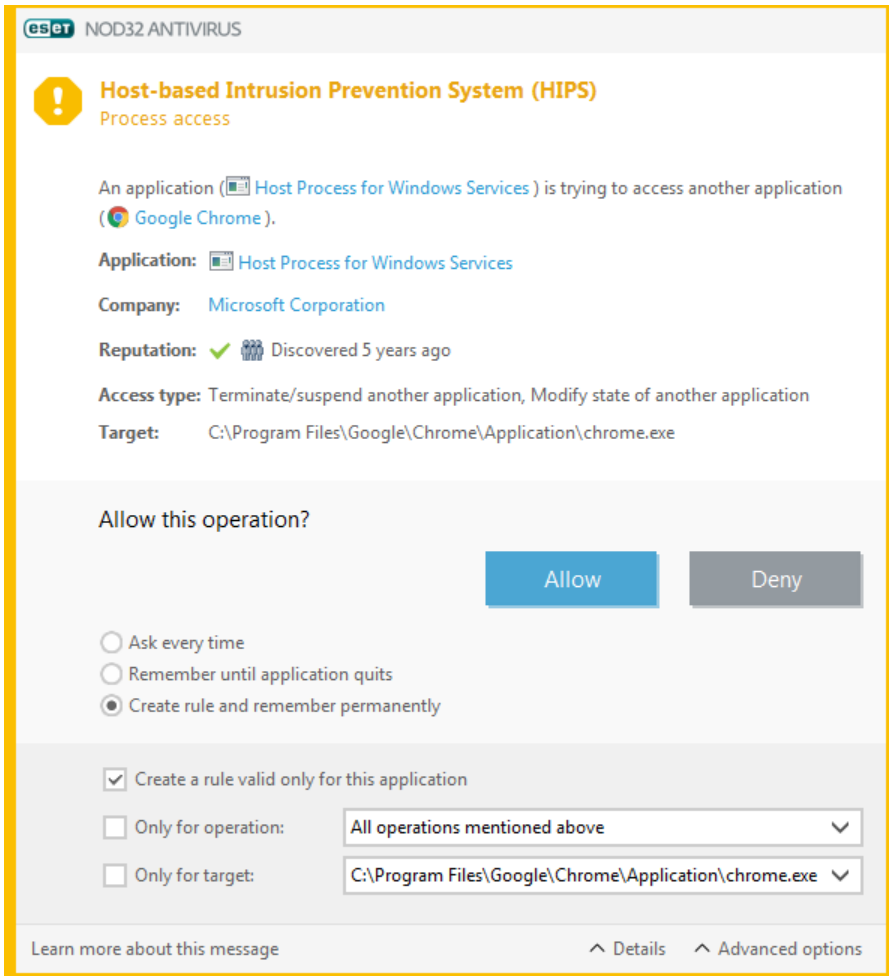
Log all blocked operations – All blocked operations will be written to the HIPS log.

Notify when changes occur in Startup applications – Displays a desktop notification each time an application is added to or removed from system startup.

Please see the our Knowledgebase article for an updated version of this help page.

4.1.4.2 HIPS interactive window

If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered. You can choose to **Deny** or **Allow** the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

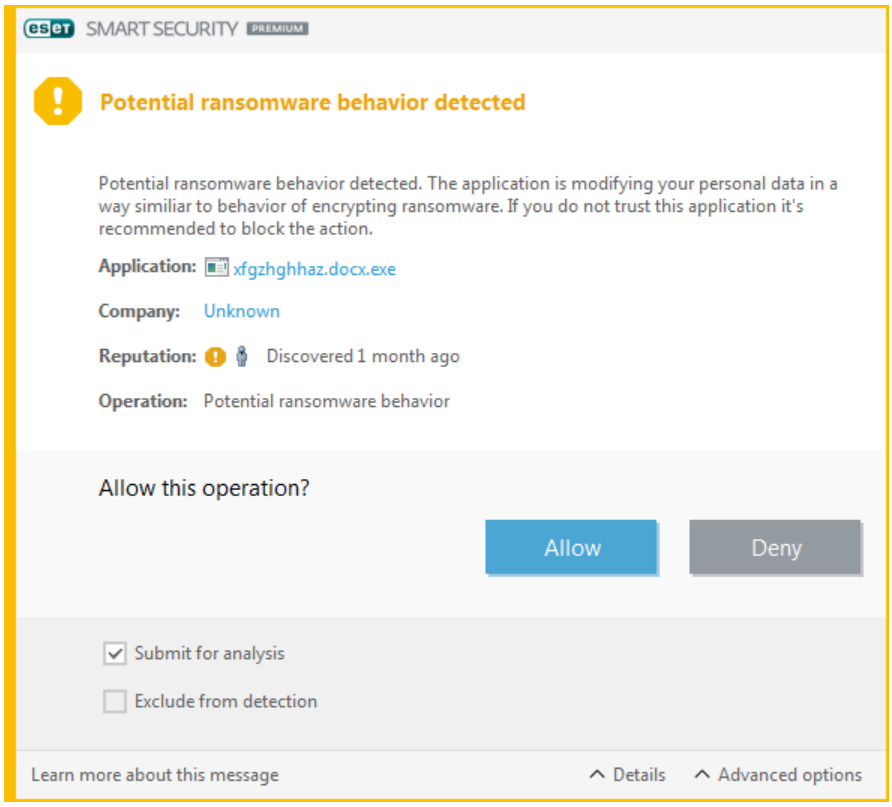

NOD32 ANTIVIRUS
Host-based Intrusion Prevention System (HIPS)
Process access
An application (Host Process for Windows Services) is trying to access another application (Google Chrome).
Application: Host Process for Windows Services
Company: Microsoft Corporation
Reputation: Discovered 5 years ago
Access type: Terminate/suspend another application, Modify state of another application
Target: C:\Program Files\Google\Chrome\Application\chrome.exe
Allow this operation?
Allow
Deny
Ask every time
Remember until application quits
Create rule and remember permanently
Create a rule valid only for this application
Only for operation:
All operations mentioned above
Only for target:
C:\Program Files\Google\Chrome\Application\chrome.exe
Learn more about this message
Details
Advanced options

The dialog window allows you to create a rule based on any new action that HIPS detects and then define the conditions under which to allow or deny that action. Settings for the exact parameters can be accessed by clicking **Details**. Rules created like this are considered equal to rules created manually, so a rule created from a dialog window can be less specific than the rule that triggered that dialog window. This means that after creating such a rule, the same operation can trigger the same window.

Remember until application quits causes the action (**Allow/Deny**) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

4.1.4.3 Potential ransomware behavior detected

This interactive window will appear when potential ransomware behavior is detected. You can choose to **Deny** or **Allow** the operation.


SMART SECURITY PREMIUM
Potential ransomware behavior detected
Potential ransomware behavior detected. The application is modifying your personal data in a way similiar to behavior of encrypting ransomware. If you do not trust this application it's recommended to block the action.
Application: xfgzhghhaz.docx.exe
Company: Unknown
Reputation: Discovered 1 month ago
Operation: Potential ransomware behavior
Allow this operation?
Allow
Deny
Submit for analysis
Exclude from detection
Learn more about this message
Details
Advanced options

The dialog window allows you **submit the file for analysis** or **exclude from detection**. Click **Details** to view specific detection parameters.

4.1.5 Gamer mode

Gamer mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. Gamer mode can also be used during presentations that cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled and the activity of the scheduler will be stopped completely. System protection still runs in the background but does not demand any user interaction.

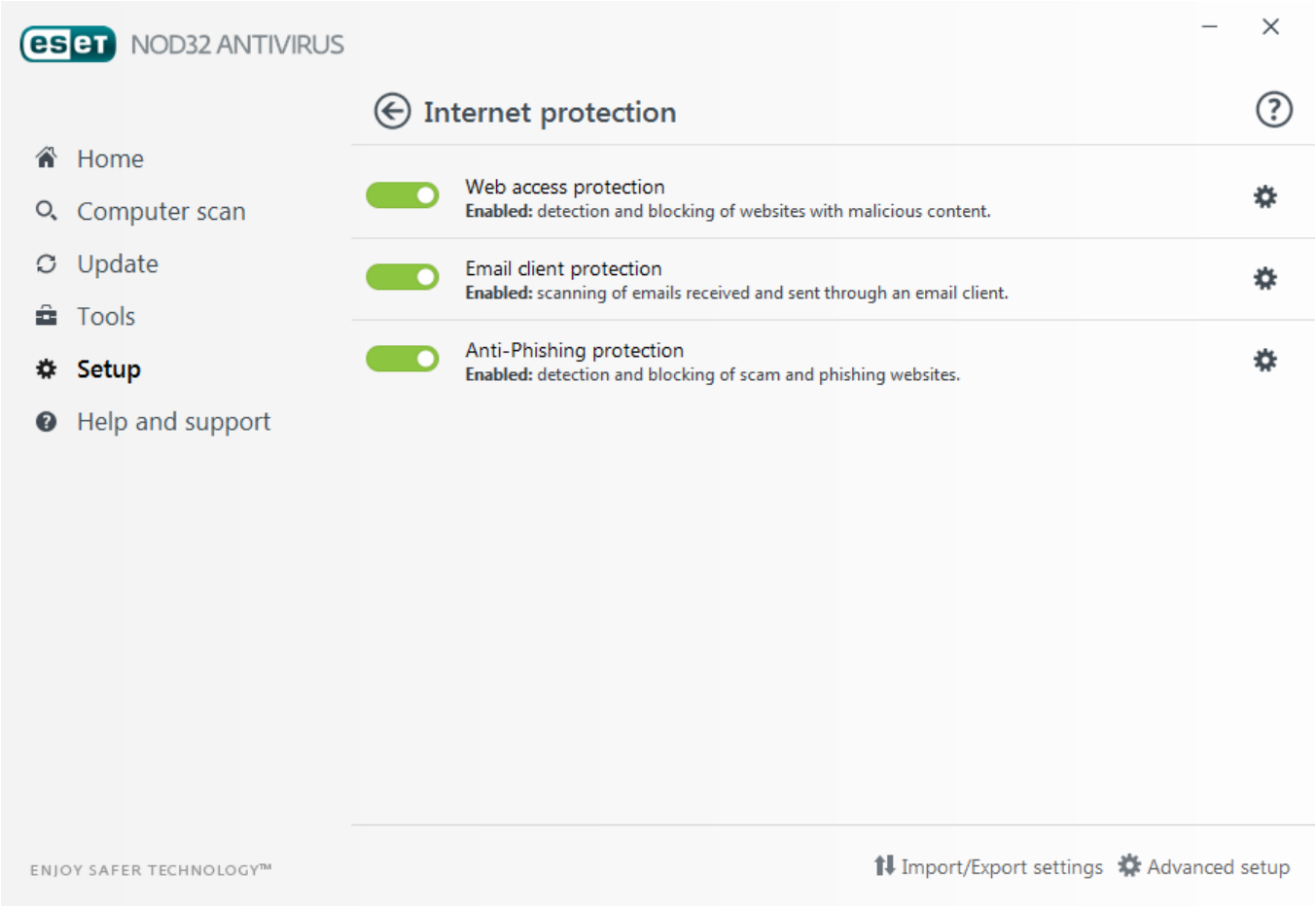
You can enable or disable Gamer mode in the main program window under **Setup** > **Computer protection** by clicking or next to **Gamer mode**. Enabling Gamer mode is a potential security risk, so the protection status icon in the taskbar will turn orange and display a warning. You will also see this warning in the main program window where you will see **Gamer mode active** in orange.

Activate **Enable Gamer mode when running applications in full-screen mode automatically** under **Advanced setup** (F5) > **Tools** to have Gamer mode start whenever you initiate a full-screen application and stop after you exit the application.

Activate **Disable Gamer mode automatically after** to define the amount of time after which Gamer mode will automatically be disabled.

4.2 Internet protection

Web and email configuration can be found in the **Setup** pane by clicking **Internet protection**. From here you can access more detailed program settings.



Internet connectivity is a standard feature for personal computers. Unfortunately, the Internet has become the primary medium for distributing malicious code. For this reason it is essential that you carefully consider your **Web access protection** settings.

Click ⚙ to open web/email/anti-phishing protection settings in Advanced setup.

Email client protection provides control of email communications received through POP3 and IMAP protocols. Using the plug-in program for your email client, ESET NOD32 Antivirus provides control of all communications to and from your email client (POP3, MAPI, IMAP, HTTP).

Anti-Phishing protection allows you to block web pages known to distribute phishing content. We strongly recommend that you leave Anti-Phishing enabled.

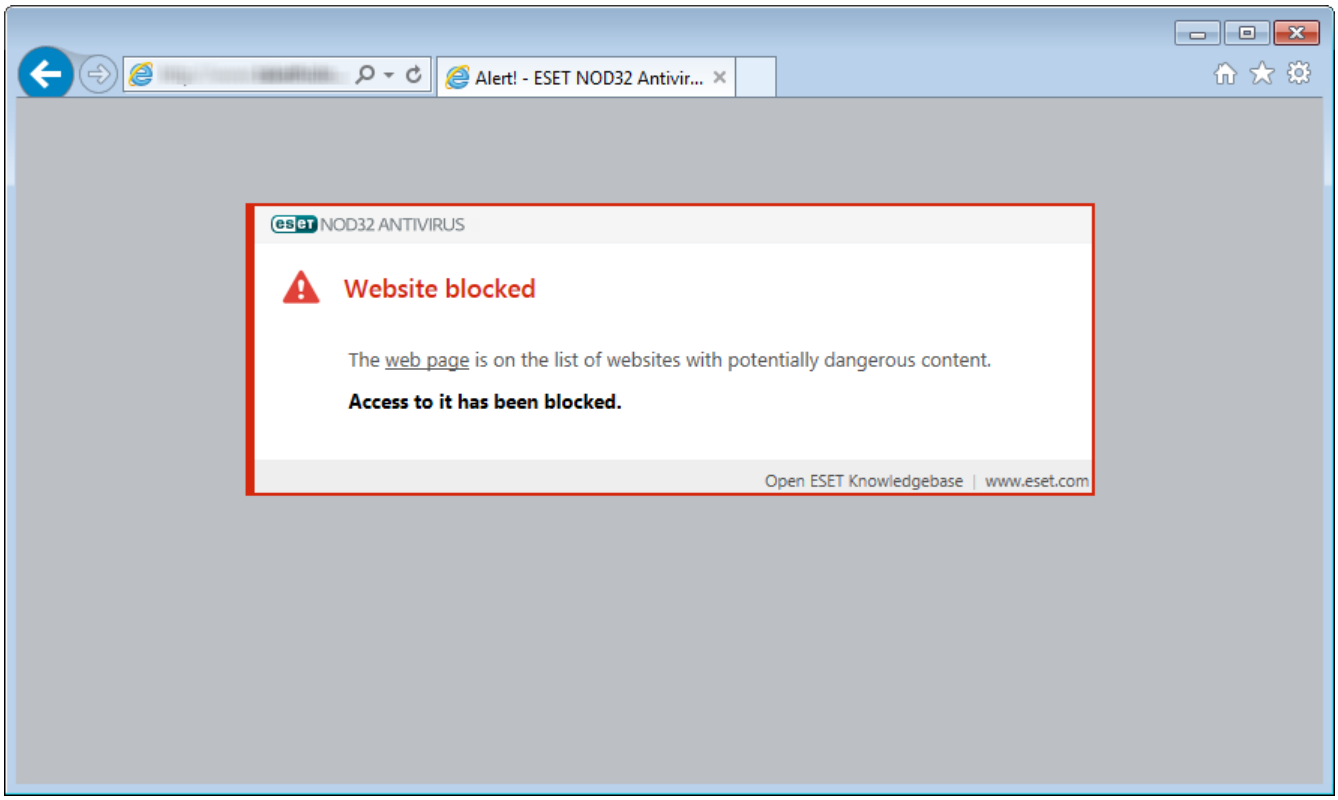
You can disable the web/email/anti-phishing protection module temporarily by clicking .

4.2.1 Web access protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Web access protection works by monitoring communication between web browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules.

Access to web pages known to contain malicious content is blocked before content is downloaded. All other webpages are scanned by the ThreatSense scanning engine when they are loaded and blocked if malicious content is detected. Web access protection offers two level of protection, blocking by blacklist and blocking by content.

We strongly recommend that Web access protection is enabled. This option can be accessed from the main window of ESET NOD32 Antivirus by navigating to **Setup** > **Internet protection** > **Web access protection**.


Alert! - ESET NOD32 Antivir...
NOD32 ANTIVIRUS
Website blocked
The web page is on the list of websites with potentially dangerous content.
Access to it has been blocked.
Open ESET Knowledgebase | www.eset.com

The following options are available in **Advanced setup** (F5) > **Web and email** > **Web access protection**:

- **Web protocols** – enables you to configure monitoring for these standard protocols which are used by most Internet browsers.
- **URL address management** – enables you to specify HTTP addresses to block, allow or exclude from checking.
- **ThreatSense parameters** – Advanced virus scanner setup – enables you to configure settings such as types of objects to scan (emails, archives, etc.), detection methods for Web access protection etc.

4.2.1.1 Basic

Enable Web access protection – When disabled, Web access protection and Anti-Phishing protection will not run.

Enable advanced scanning of browser scripts – When enabled, all JavaScript programs executed by internet browsers will be checked by antivirus scanner.

NOTE
We strongly recommend you leave Web access protection enabled.

4.2.1.2 Web protocols

By default, ESET NOD32 Antivirus is configured to monitor the HTTP protocol used by most Internet browsers.

HTTP Scanner setup

In Windows Vista and later, HTTP traffic is always monitored on all ports for all applications. In Windows XP, you can modify the **Ports used by HTTP protocol** in **Advanced setup** (F5) > **Web and email** > **Web access protection** > **Web protocols**. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

HTTPS Scanner setup

ESET NOD32 Antivirus also supports HTTPS protocol checking. HTTPS communication uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communication utilizing the SSL

(Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version.

Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL/TLS in Advanced setup section, click **Web and email** > **SSL/TLS** and enable the **Enable SSL/TLS protocol filtering** option.

4.2.1.3 URL address management

The URL address management section enables you to specify HTTP addresses to block, allow or exclude from checking.

Websites in the **List of blocked addresses** will not be accessible unless they are also included in the **List of allowed addresses**. Websites in the **List of addresses excluded from checking** are not scanned for malicious code when accessed.

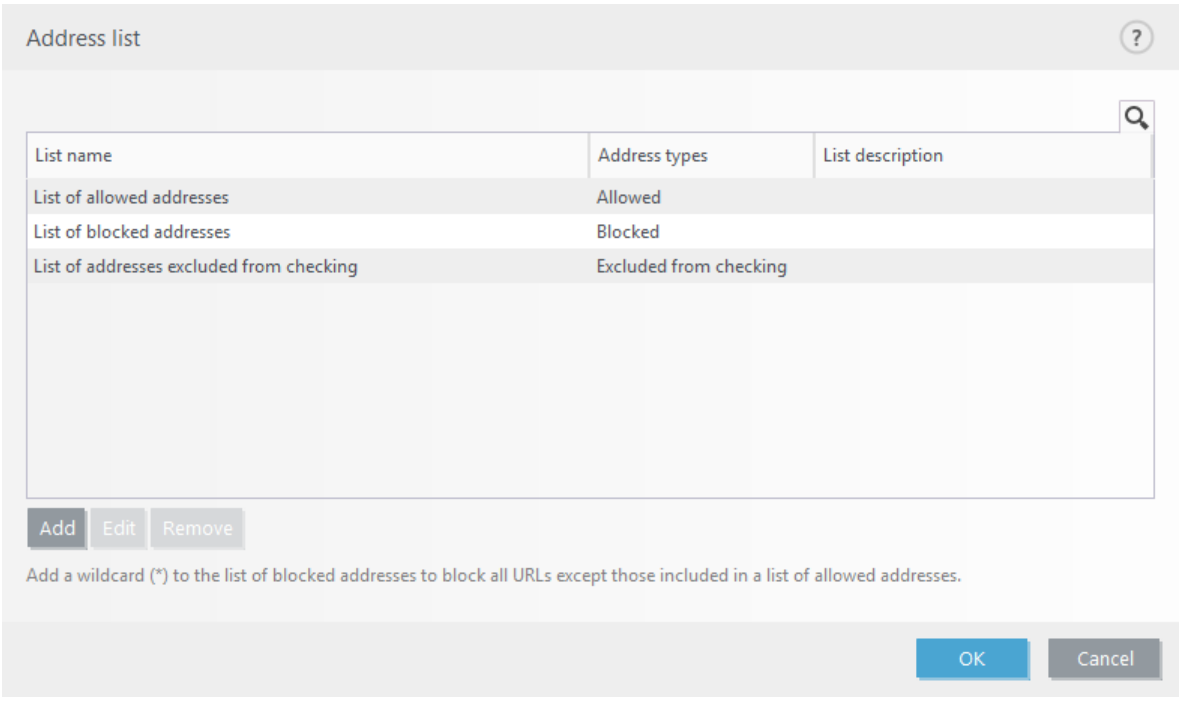
Enable SSL/TLS protocol filtering must be selected if you want to filter HTTPS addresses in addition to HTTP web pages. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

If you add a URL address to the **List of addresses excluded from filtering**, the address will be excluded from scanning. You can also allow or block certain addresses by adding them to the **List of allowed addresses** or **List of blocked addresses**.

If you want to block all HTTP addresses except addresses present in the active **List of allowed addresses**, add * to the active **List of blocked addresses**.

The special symbols * (asterisk) and ? (question mark) can be used in lists. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. See Add HTTP address / domain mask for how a whole domain including all subdomains can be matched safely. To activate a list, select **List active**. If you want to be notified when entering an address from the current list, select **Notify when applying**.

NOTE
URL address management also allows you to block or allow the opening of specific file types during internet browsing. For example, if you do not want executable files to be opened, select the list where you want to block these files from the drop-down menu and then enter the mask "**.exe".



Control elements

Add – Creates a new list in addition to the predefined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from an external public blacklist, and a second one may contain your own blacklist, making it easier to update the external list while keeping yours intact.

Edit – Modifies existing lists. Use this to add or remove addresses.

Remove – Deletes existing lists. Only available for lists created with **Add**, not for default lists.

4.2.2 Email client protection

4.2.2.1 Email clients

Integration of ESET NOD32 Antivirus with your email client increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET NOD32 Antivirus. When integrated into your email client, the ESET NOD32 Antivirus toolbar is inserted directly into the email client (the toolbar for newer versions of Windows Live Mail is not inserted), for more efficient email protection. Integration settings are located under **Advanced setup** (F5) > **Web and email** > **Email client protection** > **Email clients**.

Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

Turn on **Disable checking upon inbox content change** if you experience system slowdown when working with MS Outlook. This can occur when retrieving email from the Kerio Outlook Connector Store.

Email to scan

Enable email protection by client plugins – When email client protection by email client is disabled, email client protection by protocol filtering will be still enabled.
Received email – Toggles checking of received messages.
Sent email – Toggles checking of sent messages.
Read email – Toggles checking of read messages.

Action to be performed on infected email

No action – If enabled, the program will identify infected attachments, but will leave emails without taking any action.
Delete email – The program will notify the user about infiltration(s) and delete the message.
Move email to the Deleted items folder – Infected emails will be moved automatically to the Deleted items folder.
Move email to folder – Infected emails will be moved automatically to the specified folder.

Folder – Specify the custom folder where you want to move infected emails when detected.

Repeat scan after update – Toggles rescanning after a virus signature database update.

Accept scan results from other modules – If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

NOTE

We recommend that you enable **Enable email protection by client plugins** and **Enable email protection by protocol filtering**. These settings are located under Advanced setup (**F5**) > **Web and email** > **Email client protection** > **Email protocols**).

4.2.2.2 Email protocols

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another Internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET NOD32 Antivirus provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client.

The protection module providing this control is automatically initiated at system startup and is then active in memory. IMAP protocol control is performed automatically without the need to reconfigure the email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

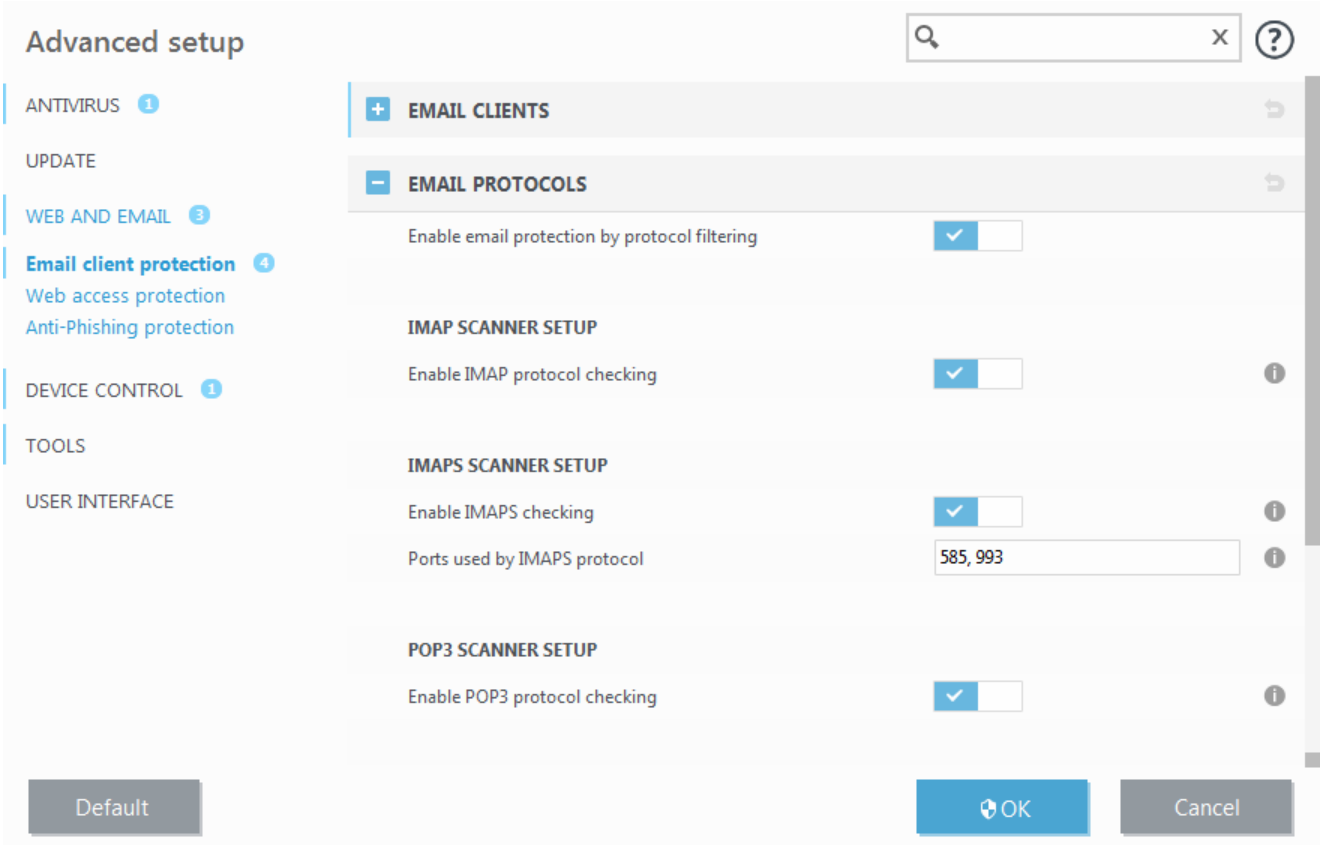
You can configure IMAP/IMAPS and POP3/POP3S protocol checking in Advanced setup. To access this setting, expand **Web and email** > **Email client protection** > **Email protocols**.

Enable email protection by protocol filtering – Enables checking of email protocols.

In Windows Vista and later, IMAP and POP3 protocols are automatically detected and scanned on all ports. In Windows XP, only the configured **Ports used by the IMAP/POP3 protocol** are scanned for all applications, and all ports are scanned for applications marked as Web and email clients.

ESET NOD32 Antivirus also supports the scanning of IMAPS and POP3S protocols, which use an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by IMAPS/POP3S protocol**, regardless of operating system version.

Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL/TLS in Advanced setup section, click **Web and email** > **SSL/TLS** and enable the **Enable SSL/TLS protocol filtering** option.



4.2.2.3 Alerts and notifications

Email protection provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other email clients, ESET NOD32 Antivirus provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.

The options for this functionality are available in **Advanced setup** under **Web and email** > **Email client protection** > **Alerts and notifications**.

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read mail**, **Append note to the subject of received and read infected email** or **Append tag messages to sent mail**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The following options are available:

- **Never** – No tag messages will be added.
- **To infected email only** – Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** – The program will append messages to all scanned email.

Append note to the subject of sent infected email – Disable this if you do not want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient. If an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

Template added to the subject of infected email – Edit this template if you want to modify the subject prefix format of an infected email. This function will replace the message subject *"Hello"* with a given prefix value *"[virus]"* to the following format: *"[virus] Hello"*. The variable *%VIRUSNAME%* represents the detected threat.

4.2.2.4 Integration with email clients

Integration of ESET NOD32 Antivirus with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET NOD32 Antivirus. When integration is activated, the ESET NOD32 Antivirus toolbar is inserted directly into the email client, allowing for more efficient email protection. Integration settings are available through **Setup** > **Advanced setup** > **Web and email** > **Email client protection** > **Email clients**.

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Select the check box next to **Disable checking upon inbox content change** if you are experiencing a system slowdown when working with your email client. This can occur when retrieving email from the Kerio Outlook Connector Store.

Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

4.2.2.4.1 Email client protection configuration

The Email client protection module supports the following email clients: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner.

4.2.2.5 POP3, POP3S filter

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET NOD32 Antivirus provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 protocol checking is performed automatically without requiring re-configuration of the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL/TLS in Advanced setup section, click **Web and email** > **SSL/TLS** and enable the **Enable SSL/TLS protocol filtering** option.

In this section, you can configure POP3 and POP3S protocol checking.

Enable POP3 protocol checking – If enabled, all traffic through POP3 is monitored for malicious software.

Ports used by POP3 protocol – A list of ports used by the POP3 protocol (110 by default).

ESET NOD32 Antivirus also supports POP3S protocol checking. This type of communication uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communications utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) encryption methods.

Do not use POP3S checking – Encrypted communication will not be checked.

Use POP3S protocol checking for selected ports – Check this option to enable POP3S checking only for ports defined in **Ports used by POP3S protocol**.

Ports used by POP3S protocol – A list of POP3S ports to check (995 by default).

4.2.3 Protocol filtering

Antivirus protection for application protocols is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. To edit encrypted (SSL/TLS) settings, go to **Web and email** > **SSL/TLS**.

Enable application protocol content filtering – Can be used to disable protocol filtering. Note that many ESET NOD32 Antivirus components (Web access protection, Email protocols protection, Anti-Phishing, Web control) depend on this and will be non-functional without it.

Excluded applications – Allows you to exclude specific applications from protocol filtering. Useful when protocol filtering causes compatibility issues.

Excluded IP addresses – Allows you to exclude specific remote addresses from protocol filtering. Useful when protocol filtering causes compatibility issues.

Web and email clients – Used only on Windows XP operating systems, allows you to select applications for which all traffic is filtered by protocol filtering, regardless of ports used.

4.2.3.1 Web and email clients

NOTE
Starting with Windows Vista Service Pack 1 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since WFP technology uses special monitoring techniques, the **Web and email clients** section is not available.

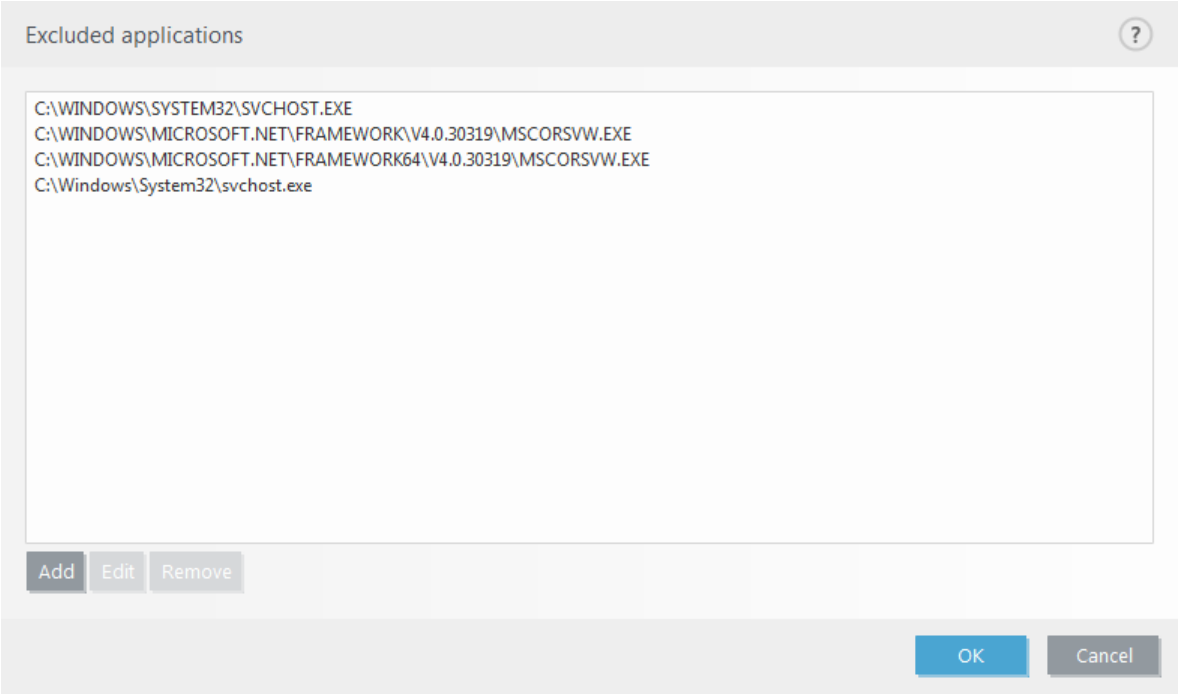
Because of the enormous amount of malicious code circulating the Internet, safe Internet browsing is a very important aspect of computer protection. Web browser vulnerabilities and fraudulent links help malicious code enter the system unnoticed which is why ESET NOD32 Antivirus focuses on web browser security. Each application accessing the network can be marked as an Internet browser. The check box is two-state:

- **Deselected** – Communication of applications is filtered only for specified ports.
- **Selected** – Communication is always filtered (even if a different port is set).

4.2.3.2 Excluded applications

To exclude communication of specific network-aware applications from content filtering, select them in the list. HTTP/POP3/IMAP communication of the selected applications will not be checked for threats. We recommend only using this for applications that do not work properly with their communication being checked.

Running applications and services will be available here automatically. Click **Add** to add an application manually if it is not shown on the protocol filtering list.

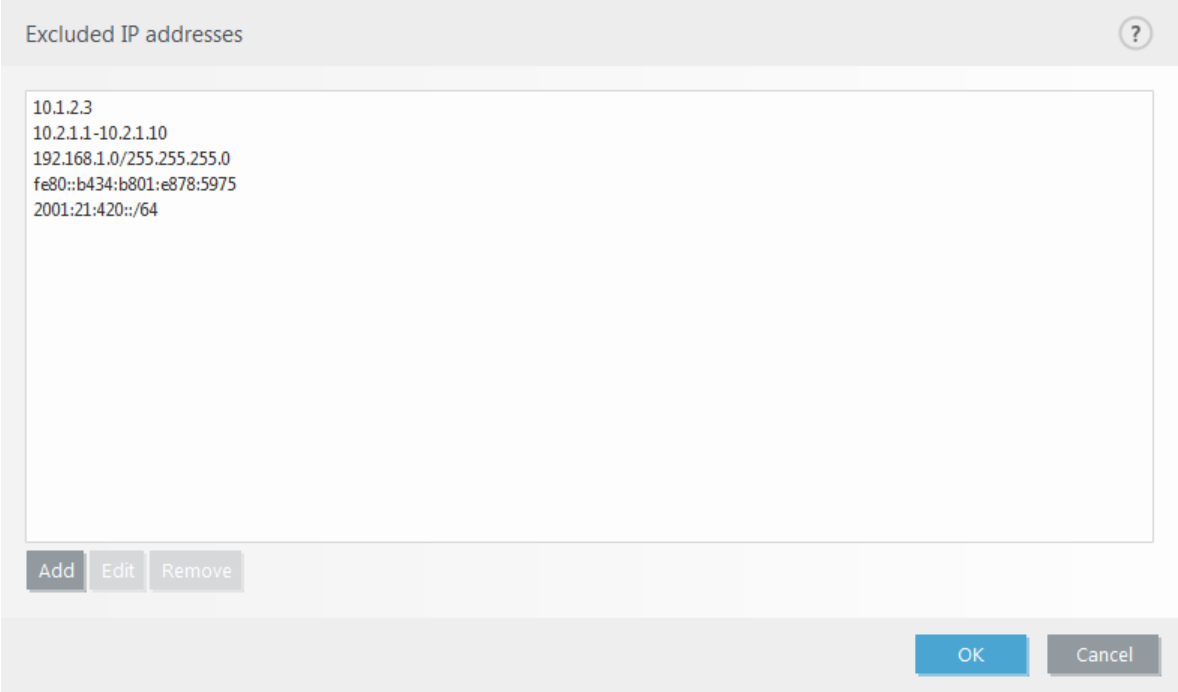


4.2.3.3 Excluded IP addresses

The entries in the list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Click **Add** to exclude an IP address/address range/subnet of a remote point not shown on the protocol filtering list.

Click **Remove** to remove selected entries from the list.



4.2.3.3.1 Add IPv4 address

This allows you to add an IP address/address range/subnet of a remote point to which a rule is applied. Internet Protocol version 4 is the older but still the most widely used.

Single address – Adds the IP address of an individual computer for which the rule is to be applied (for example *192.168.0.10*).

Address range – Enter the starting and ending address IP address to specify the IP range (of several computers) for which the rule is to be applied (for example *192.168.0.1* to *192.168.0.99*).

Subnet – Subnet (a group of computers) defined by an IP address and mask.

For example, *255.255.255.0* is the network mask for the *192.168.1.0/24* prefix, that means *192.168.1.1* to *192.168.1.254* address range.

4.2.3.3.2 Add IPv6 address

This allows you to add an IPv6 address/subnet of a remote point for which the rule is applied. It is the newest version of the Internet protocol and will replace the older version 4.

Single address – Adds the IP address of an individual computer for which the rule is to be applied (for example *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnet – Subnet (a group of computers) is defined by an IP address and mask (for example: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus is capable of checking for threats in communications that use the SSL protocol. You can use various scanning modes to examine SSL protected communications with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering – If protocol filtering is disabled, the program will not scan communications over SSL.

SSL/TLS protocol filtering mode is available in following options:

Automatic mode – Default mode will only scan appropriate applications such as web browsers and email clients. You can override it by selecting applications for which their communications will be scanned.

Interactive mode – If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL certificates / applications that will be excluded from scanning.

Policy mode – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

List of SSL filtered applications – Allows you to customize ESET NOD32 Antivirus behavior for specific applications.

List of known certificates – Allows you to customize ESET NOD32 Antivirus behavior for specific SSL certificates.

Exclude communication secured with Extended Validation Certificates (EV) – When enabled, communication with this type of SSL certificate will be excluded from checking. Extended Validation SSL Certificates assure that you are really viewing your website and not a fake site that looks exactly like yours (typical for phishing sites).

Block encrypted communication utilizing the obsolete protocol SSL v2 – Communication using the earlier version of the SSL protocol will automatically be blocked.

Root certificate

Add the root certificate to known browsers – For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). When enabled, ESET NOD32 Antivirus will automatically add the ESET root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and manually import it into the browser.

Certificate validity

If the certificate cannot be verified using the TRCA certificate store – In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store. This means that the certificate is signed by someone (for example, the administrator of a web server or a small business) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by the TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. You can select **Block communication that uses the certificate** to always terminate encrypted connections to sites with unverified certificates.

If the certificate is invalid or corrupt – This means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave **Block communication that uses the certificate** selected.

4.2.3.4.1 Certificates

For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). **Add the root certificate to known browsers** should be enabled. Select this option to automatically add the ESET root certificate to the known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (e.g. Internet Explorer). To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and then manually import it into the browser.

In some cases, the certificate cannot be verified using the Trusted Root Certification Authorities store (e.g. VeriSign). This means that the certificate is self-signed by someone (e.g. administrator of a web server or a small business company) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. An action selection dialog will be displayed where you can decide to mark the certificate as trusted or excluded. If the certificate is not present in the TRCA list, the window is red. If the certificate is on the TRCA list, the window will be green.

You can select **Block communication that uses the certificate** to always terminate an encrypted connection to the site that uses the unverified certificate.

If the certificate is invalid or corrupt, it means that the certificate expired or was incorrectly self-signed. In this case, we recommend that you block the communication that uses the certificate.

4.2.3.4.1.1 Encrypted network traffic

If the computer is configured for SSL protocol scanning, a dialog window prompting you to choose an action may be opened when there is an attempt to establish encrypted communication (using an unknown certificate).

The dialog window contains the following information:

- name of the application that initiated the communication
- name of the certificate used
- action to perform - whether to scan the encrypted communication and whether to remember the action for the application / certificate

If the certificate is not located in the Trusted Root Certification Authorities store (TRCA), it is considered untrusted.

4.2.3.4.2 List of known certificates

The **List of known certificates** can be used to customize ESET NOD32 Antivirus behavior for specific SSL certificates, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**. The list can be viewed and edited in **Advanced setup** (F5) > **Web and email** > **SSL/TLS** > **List of known certificates**.

The **List of known certificates** window consists of:

Columns

Name – Name of the certificate.

Certificate issuer – Name of the certificate creator.

Certificate subject – The subject field identifies the entity associated with the public key stored in the subject public key field.

Access – Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to always ask user what to do.

Scan – Select **Scan** or **Ignore** as the **Scan action** to scan or ignore communication secured by this certificate. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add – Add a new certificate and adjust its settings regarding access and scan options.

Edit – Select the certificate that you want to configure and click **Edit**.

Remove – Select the certificate that you want to delete and click **Remove**.

OK/Cancel – Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

4.2.3.4.3 List of SSL/TLS filtered applications

The **List of SSL/TLS filtered applications** can be used to customize ESET NOD32 Antivirus behavior for specific applications, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**. The list can be viewed and edited in **Advanced setup** (F5) > **Web and email** > **SSL/TLS** > **List of SSL/TLS filtered applications**.

The **List of SSL/TLS filtered applications** window consists of:

Columns

Application – Name of the application.

Scan action – Select **Scan** or **Ignore** to scan or ignore communication. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add – Add filtered application.

Edit – Select the certificate that you want to configure and click **Edit**.

Remove – Select the certificate that you want to delete and click **Remove**.

OK/Cancel – Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

4.2.4 Anti-Phishing protection

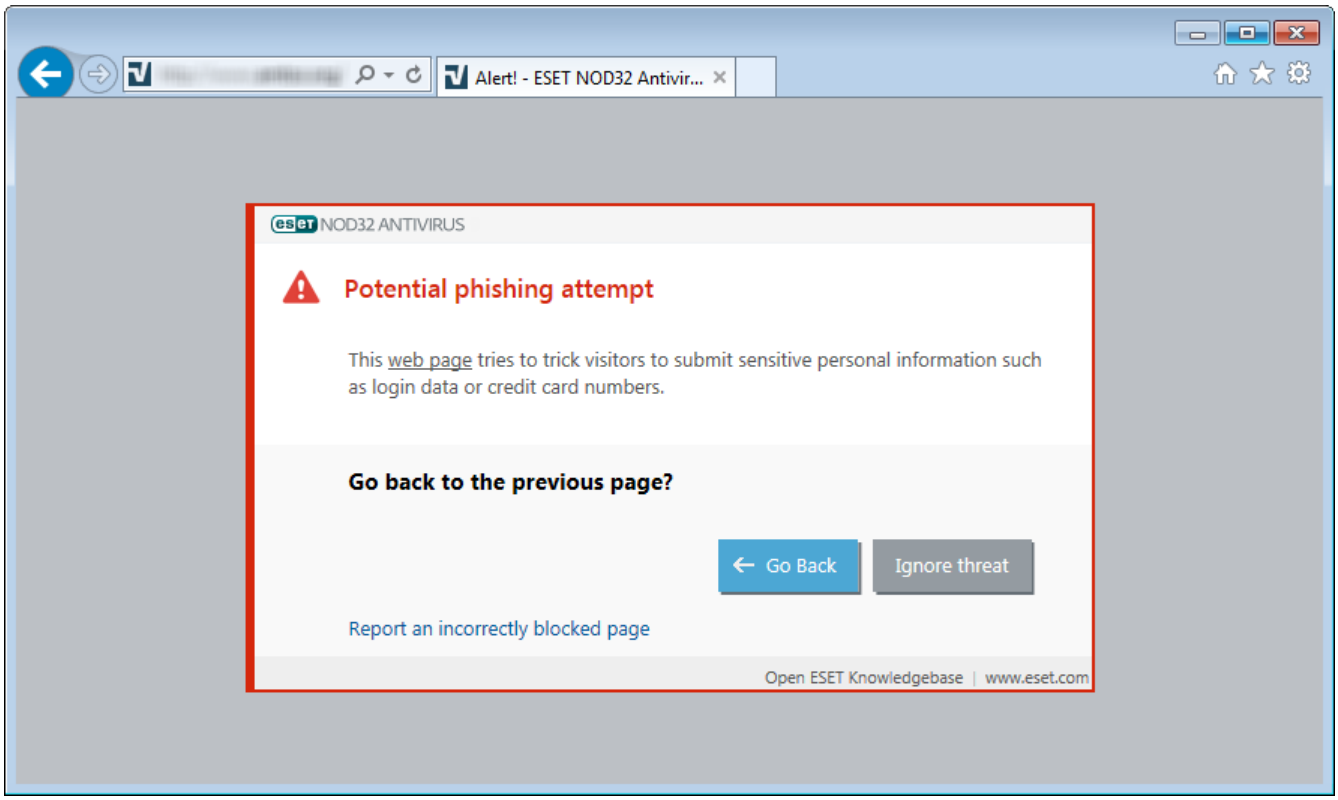
The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET NOD32 Antivirus includes anti-phishing protection, which blocks web pages known to distribute this type of content.

We strongly recommend that you enable Anti-Phishing in ESET NOD32 Antivirus. To do so, open **Advanced setup** (F5) and navigate to **Web and email** > **Anti-Phishing protection**.

Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET NOD32 Antivirus.

Accessing a phishing website

When you access a recognized phishing website, the following dialog will be displayed in your web browser. If you still want to access the website, click **Ignore threat** (not recommended).


Alert! - ESET NOD32 Antivir...
NOD32 ANTIVIRUS
Potential phishing attempt
This web page tries to trick visitors to submit sensitive personal information such as login data or credit card numbers.
Go back to the previous page?
Go Back
Ignore threat
Report an incorrectly blocked page
Open ESET Knowledgebase | www.eset.com

NOTE
Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool. From **Advanced setup** (F5) expand **Web and email** > **Web access protection** > **URL address management** > **Address list**, click **Edit** and then add the website that you want to edit to the list.

Phishing site reporting

The Report link enables you to report a phishing/malicious website to ESET for analysis.

NOTE
Before submitting a website to ESET, make sure it meets one or more of the following criteria:

- the website is not detected at all,
- the website is incorrectly detected as a threat. In this case, you can Report an incorectly blocked page.

Alternatively, you can submit the website by email. Send your email to samples@eset.com. Remember to use a descriptive subject and enclose as much information about the website as possible (for example, the website that referred you there, how you learned of this website, etc.).

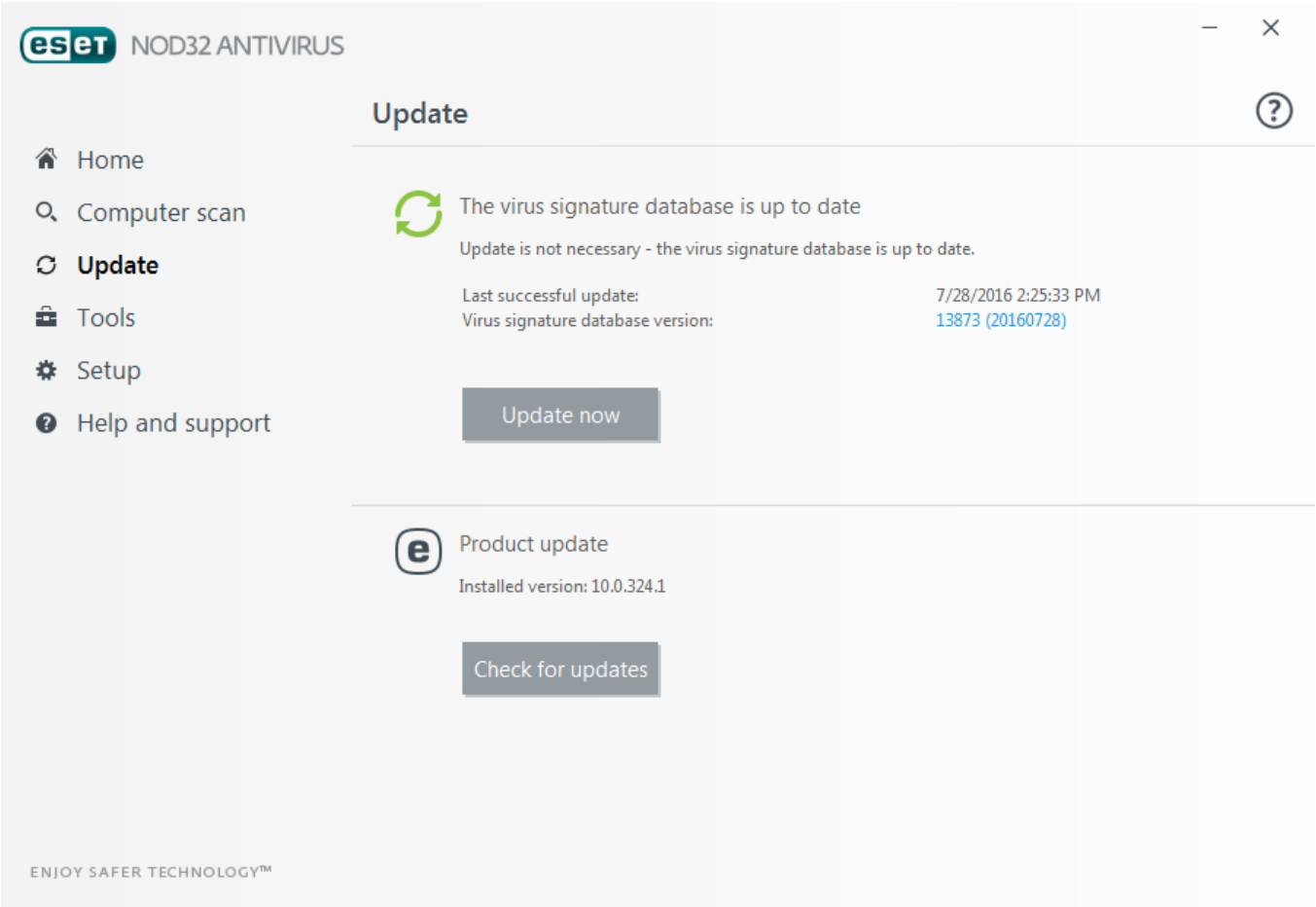
4.3 Updating the program

Regularly updating ESET NOD32 Antivirus is the best method to ensure the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways, by updating the virus signature database and by updating system components.

By clicking **Update** in the main program window, you can view current update status including the date and time of the last successful update and if an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added within the given update.

In addition to automatic updates, you can click **Update now** to trigger an update manually. Updating the virus signature database and updating program components are important parts of maintaining complete protection against malicious code. Please pay attention to their configuration and operation. You must activate your product using your License key to receive updates. If you did not do so during installation, you can enter your license key to activate your product when updating to access ESET update servers.

NOTE
Your License key is provided in an email from ESET after purchasing ESET NOD32 Antivirus.



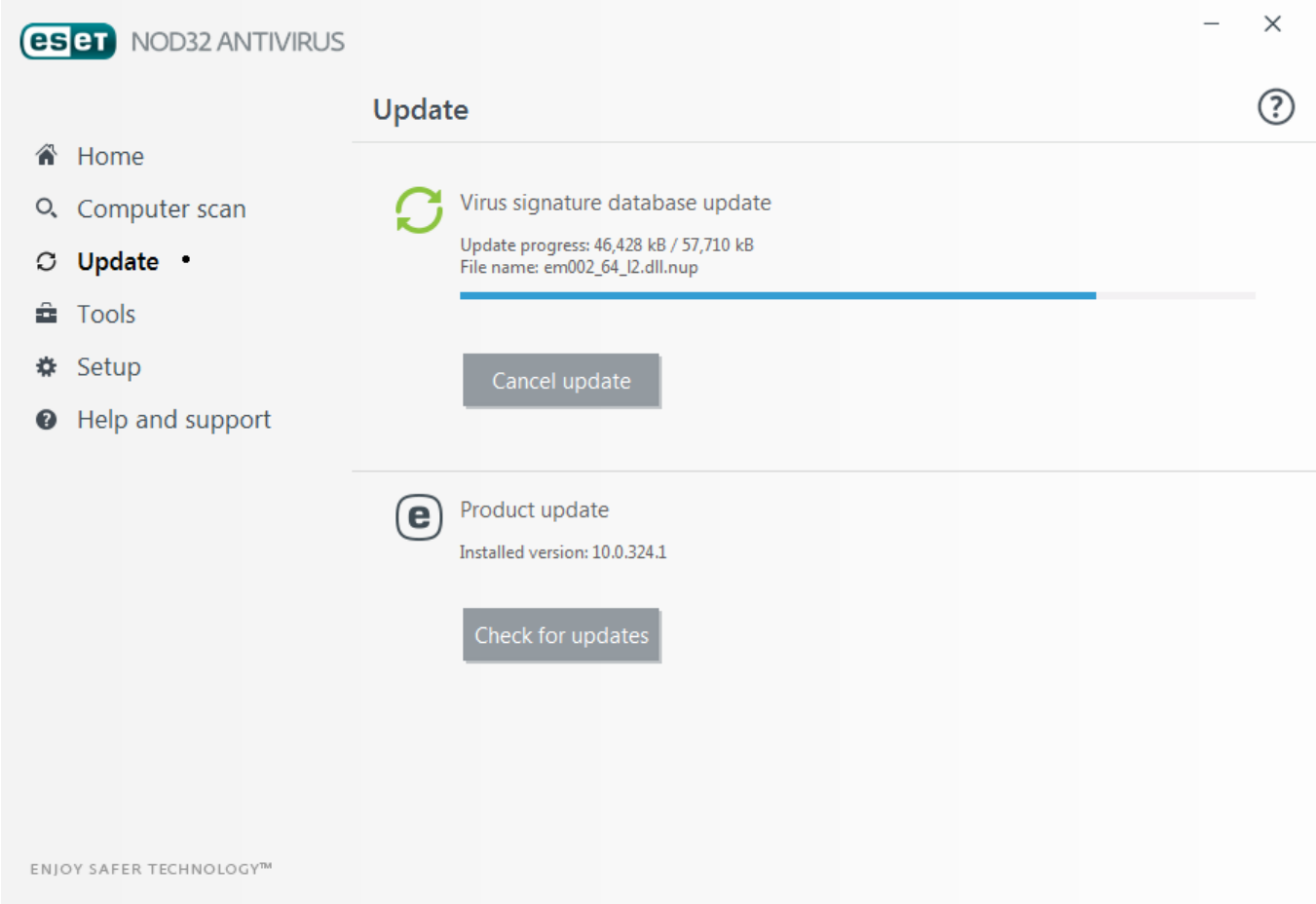
Last successful update – The date of the last update. If you do not see a recent date, your virus signature database may not be current.

Virus signature database version – The virus signature database number, which is also an active link to the ESET website. Click it to view a list of all signatures added in a given update.

Click **Check for updates** to detect the latest available version of ESET NOD32 Antivirus.

Update process

After clicking **Update now**, the download will begin. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Cancel update**.

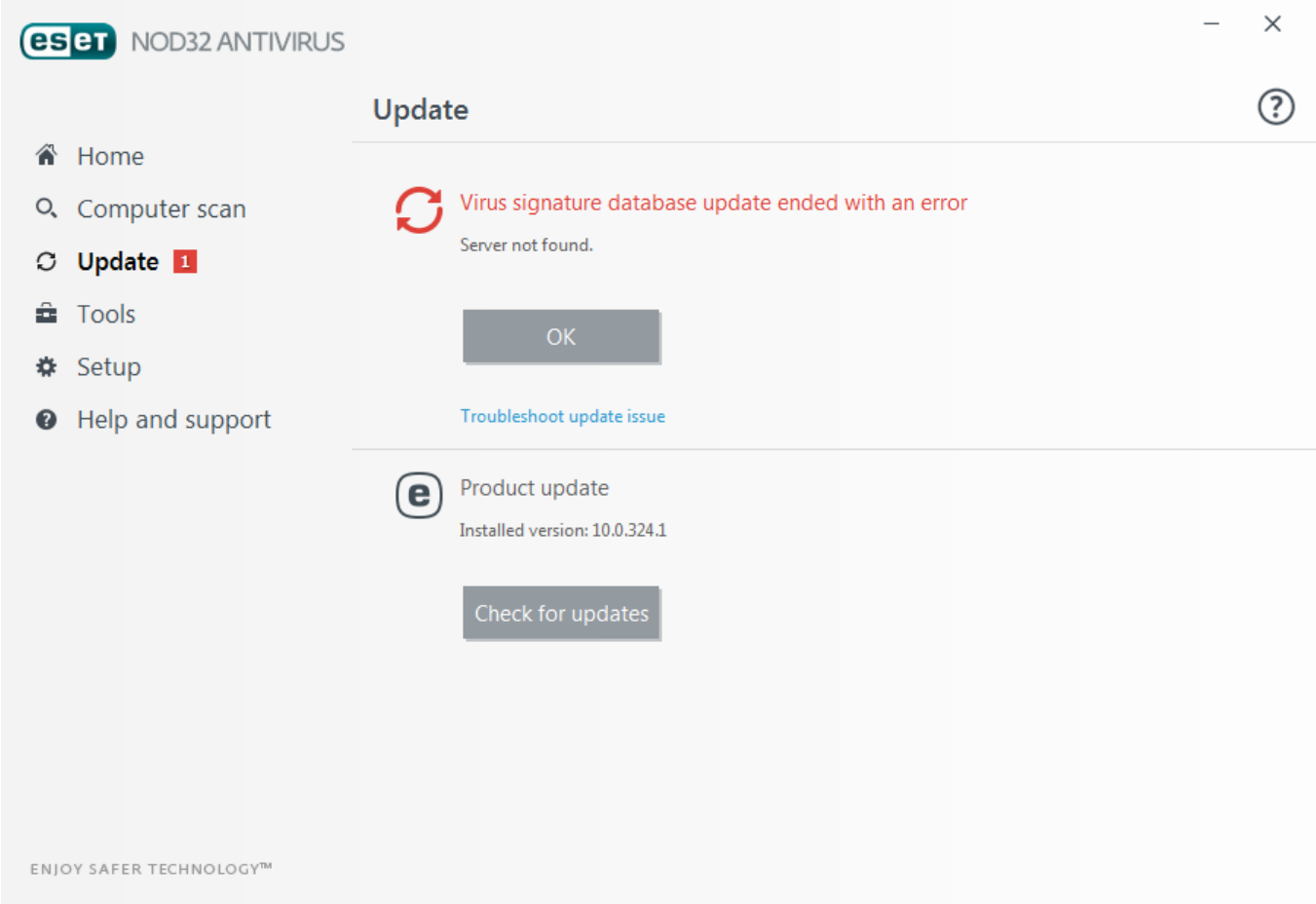


IMPORTANT

Under normal circumstances the message **Update is not necessary – the virus signature database is up to date** will appear in the **Update** window. If this is not the case, the program is out of date and more vulnerable to infection. Please update the virus signature database as soon as possible.

The previous notification is related to the following two **Virus signature database update ended with an error** messages about unsuccessful updates:

1. **Invalid license** – The license key has been incorrectly entered in update setup. We recommend that you check your authentication data. The Advanced setup window (click **Setup** from the main menu and then click **Advanced setup**, or press F5 on your keyboard) contains additional update options. Click **Help and support** > **Change license** from the main menu to enter a new license key.
2. **An error occurred while downloading update files** – This can be caused by incorrect Internet connection settings. We recommend that you check your Internet connectivity (by opening any website in your web browser). If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.



NOTE
For more information please visit this ESET Knowledgebase article.

4.3.1 Update settings

Update setup options are available in the **Advanced setup** tree (F5) under **Update** > **Basic**. This section specifies update source information like the update servers being used and authentication data for these servers.

General

The update profile that is currently in use is displayed in the **Selected profile** drop-down menu. To create a new profile, click **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**.

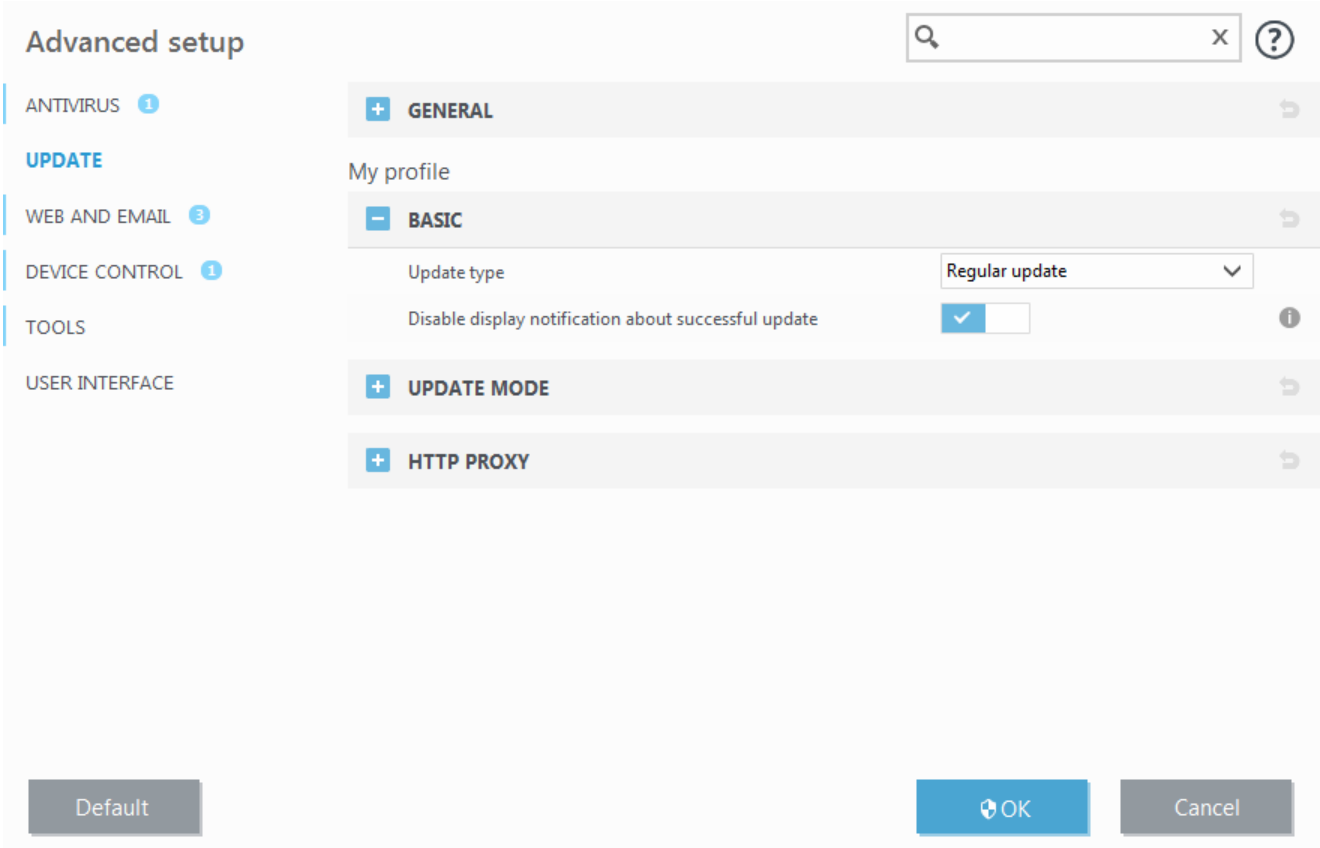
If you are experiencing difficulty when attempting to download virus signature database updates, click **Clear** to clear the temporary update files/cache.

Rollback

If you suspect that a new update of the virus database and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET NOD32 Antivirus records snapshots of virus signature database and program modules for use with the *rollback* feature. In order to create virus database snapshots, leave the **Create snapshots of update files** switch enabled. The **Number of locally stored snapshots** field defines the number of previous virus database snapshots stored.

If you click **Rollback** (**Advanced setup** (F5) > **Update** > **General**), you have to select a time interval from the drop-down menu that represents the period of time that the virus signature database and program module updates will be paused.



For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the Internet (for example, HTTP communication).

Basic

By default, the **Update type** is set to **Regular update** to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the **Pre-release update** option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required.

Disable display notification about successful update – Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running. Please note that Gamer mode will turn off all notifications.

4.3.1.1 Update profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users who need an alternative profile for Internet connection properties that regularly change.

The **Selected profile** drop-down menu displays the currently selected profile and is set to **My profile** by default. To create a new profile, click **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**.

4.3.1.2 Advanced update setup

Advanced update setup options include the configuration of **Update mode**, **HTTP Proxy**.

4.3.1.2.1 Update mode

The **Update mode** tab contains options related to regular program updates. These settings enable you to predefine program behavior when new virus signature database or program component updates are available.

Program component updates include new features or makes changes to features from previous versions, and are included as part of regular (virus signature database) updates. After a program component update has been installed, a computer restart may be required.

The following settings are available:

Application update – When enabled, each program component upgrade will be performed automatically and silently without full product upgrading.

Ask before downloading update – When this option is active, a notification will be displayed and you will be asked to confirm the installation of any available updates before they are installed.

Ask if an update file is greater than (kB) – If the update file is larger than the size specified here, a notification will be displayed and you will be asked to confirm the installation of any available updates before they are installed.

4.3.1.2.2 HTTP Proxy

To access the proxy server setup options for a given update profile, click **Update** in the **Advanced setup** tree (F5) and then click **HTTP Proxy**. Click the **Proxy mode** drop-down menu and select one of the three following options:

- Do not use proxy server
- Connection through a proxy server
- Use global proxy server settings

Select **Use global proxy server settings** to use the proxy server configuration options already specified in the **Tools** > **Proxy server** branch of the Advanced setup tree.

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET NOD32 Antivirus.

Connection through a proxy server option should be selected if:

- A different proxy server than the one defined in **Tools** > **Proxy server** is used to update ESET NOD32 Antivirus. In this configuration, information for the new proxy should be specified under **Proxy server** address, communication **Port** (3128 by default), and **Username** and **Password** for the proxy server if required.
- Proxy server settings are not set globally, but ESET NOD32 Antivirus will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. Settings are taken from Internet Explorer during program installation, but if they are changed (for example, if you change your ISP), please make sure the HTTP proxy settings listed in this window are correct. Otherwise the program will not be able to connect to update servers.

The default setting for the proxy server is **Use global proxy server settings**.

Use direct connection if proxy is not available – Proxy will be bypassed during update if it is unreachable.

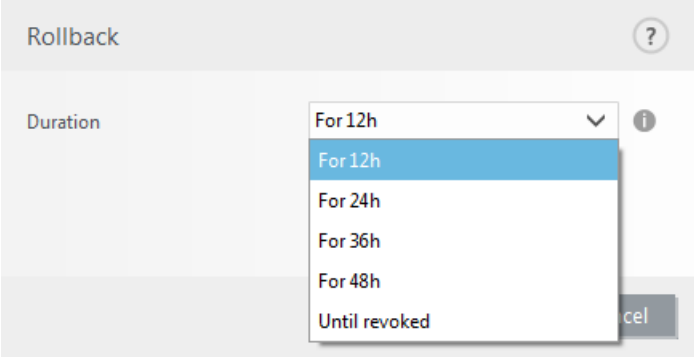
NOTE
The **Username** and **Password** fields in this section are specific to the proxy server. Complete these fields only if a username and password are required to access the proxy server. These fields are not for your ESET NOD32 Antivirus Username and password, and should only be completed if you know you need a password to access the internet via a proxy server.

4.3.2 Update rollback

If you suspect that a new update of the virus database and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

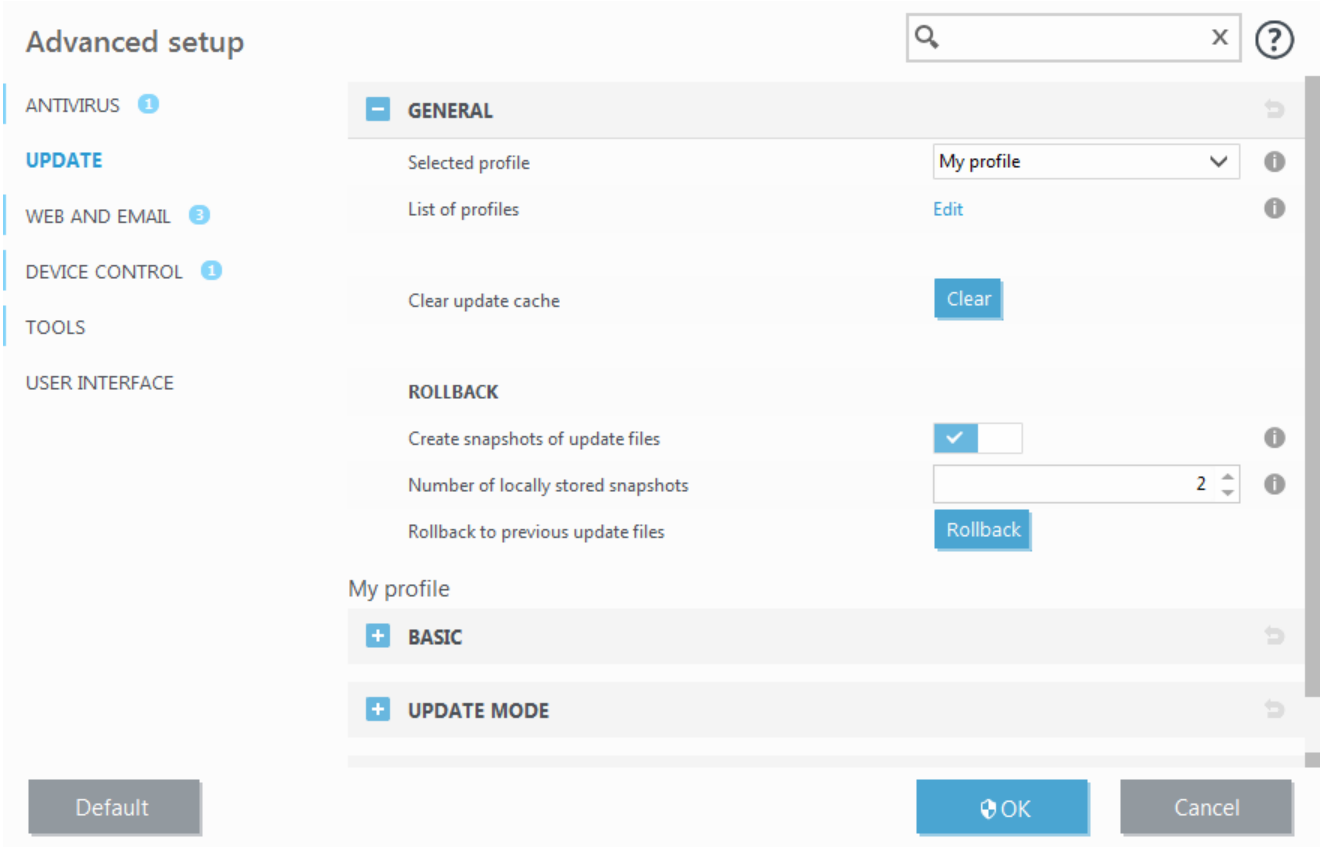
ESET NOD32 Antivirus records snapshots of virus signature database and program modules for use with the *rollback* feature. In order to create virus database snapshots, leave **Create snapshots of update files** check box selected. The **Number of locally stored snapshots** field defines the number of previous virus database snapshots stored.

If you click **Rollback** (**Advanced setup** (F5) > **Update** > **General**), you have to select a time interval from the **Duration** drop-down menu that represents the period of time that the virus signature database and program module updates will be paused.



Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. Because it represents a potential security risk, we do not recommend selecting this option.

If a rollback is performed, the **Roll back** button changes to **Allow updates**. No updates will be allowed for the time interval selected from the **Suspend updates** drop-down menu. The virus signature database version is downgraded to the oldest available and stored as a snapshot in the local computer file system.



NOTE

Let the number 6871 be the most recent version of virus signature database. 6870 and 6868 are stored as a virus signature database snapshots. Note that 6869 is not available because, for example, the computer was turned off and a more recent update was made available before 6869 was downloaded. If the **Number of locally stored snapshots** field is set to 2 and you click **Roll back**, the virus signature database (including program modules) will be restored to version number 6868. This process may take some time. Check whether the virus signature database version has downgraded from the main program window of ESET NOD32 Antivirus in the Update section.

4.3.3 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking **Update** from the main menu.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET NOD32 Antivirus:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see section Scheduler.

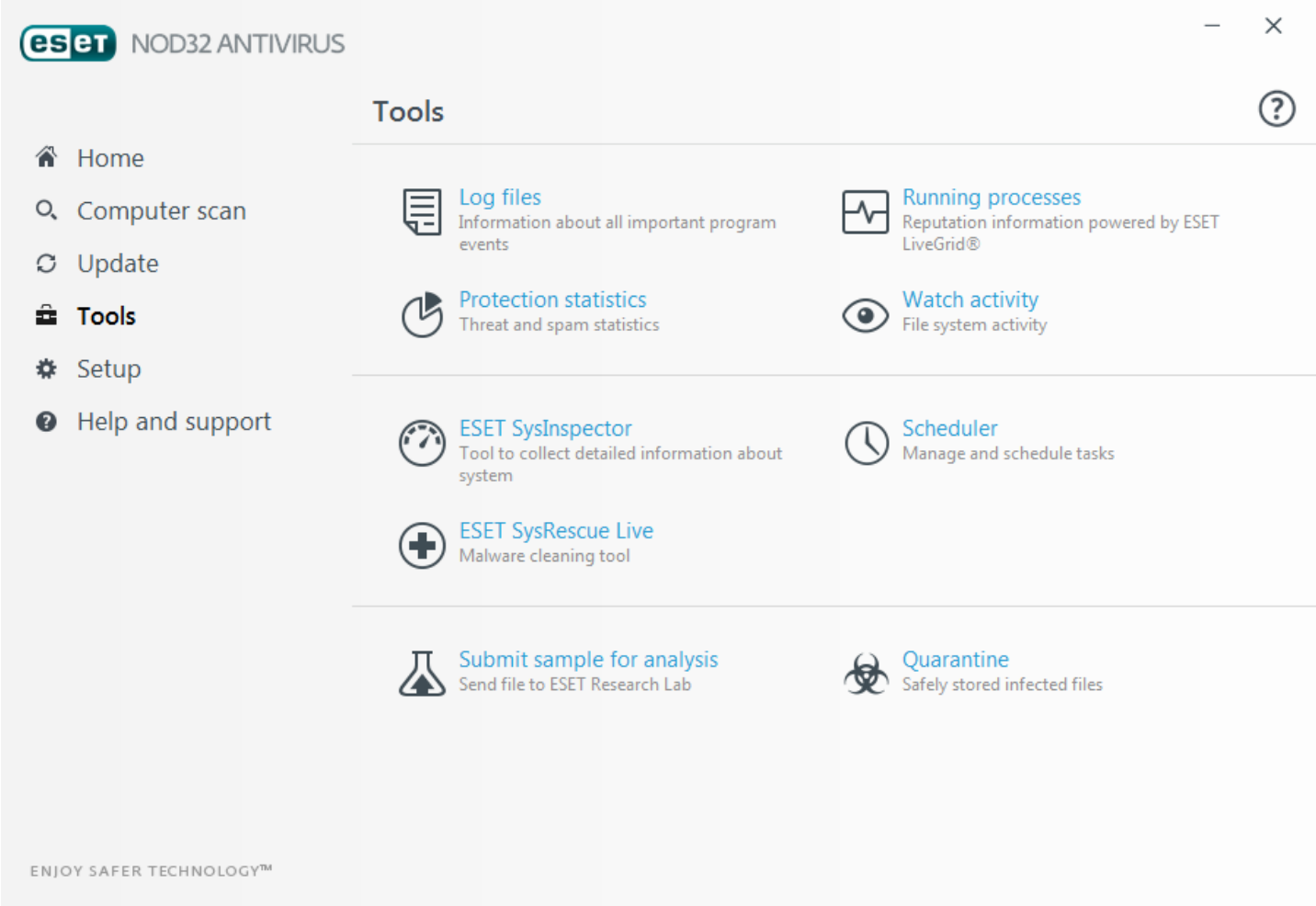
4.4 Tools

The **Tools** menu includes modules that help simplify program administration and offers additional options for advanced users.

Click More tools to display other tools to protect your computer.

4.4.1 Tools in ESET NOD32 Antivirus

The **Tools** menu includes modules that help simplify program administration and offers additional options for advanced users.



This menu includes the following tools:

Log files

Protection statistics

Watch activity

Running processes (if ESET LiveGrid® is enabled in ESET NOD32 Antivirus)

ESET SysInspector

ESET SysRescue Live – Redirects you to the ESET SysRescue Live page, where you can download the ESET SysRescue Live image or Live CD/USB Creator for Microsoft Windows operating systems.

Scheduler

Submit sample for analysis – Allows you to submit a suspicious file for analysis to the ESET Research Lab. The dialog window displayed after clicking this option is described in this section.

Quarantine

NOTE
ESET SysRescue may not be available for Windows 8 in older versions of ESET security products. In this case we recommend that you upgrade your product or create an ESET SysRescue disk on another version of Microsoft Windows.

4.4.1.1 Log files

Log files contain information about important program events that have occurred and provide an overview of detected threats. Logging is an essential part of system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view text messages and logs directly from the ESET NOD32 Antivirus environment, as well as to archive logs.

Log files are accessible from the main program window by clicking **Tools** > **Log files**. Select the desired log type from the **Log** drop-down menu. The following logs are available:

- **Detected threats** – The threat log offers detailed information about infiltrations detected by ESET NOD32 Antivirus . Log information includes the time of detection, name of infiltration, location, the action taken and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window.
- **Events** – All important actions performed by ESET NOD32 Antivirus are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed for system administrators and users to solve problems. Often the information found here can help you find a solution for a problem occurring in the program.
- **Computer scan** – Results of all completed manual or planned scans are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.
- **HIPS** – Contains records of specific HIPS rules which are marked for recording. The protocol shows the application that triggered the operation, the result (whether the rule was permitted or prohibited) and the rule name.
- **Filtered websites** – This list is useful if you want to view a list of websites that were blocked by Web access protection. Each log includes time, URL address, user and application that created a connection to a particular website.
- **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with respective Device control rules will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. You can also view details such as device type, serial number, vendor name and media size (if available).

Select the contents of any log and press **Ctrl + C** to copy it to the clipboard . Hold **Ctrl** and **Shift** to select multiple entries.

Click **Filtering** to open the **Log filtering** window where you can define filtering criteria.

Right-click a specific record to open the context menu. The following options are available in the context menu:

- **Show** – Shows more detailed information about the selected log in a new window.
- **Filter same records** – After activating this filter, you will only see records of the same type (diagnostics, warnings, ...).
- **Filter.../Find...** – After clicking this option, the Search in log window will allow you to define filtering criteria for specific log entries.
- **Enable filter** – Activates filter settings.
- **Disable filter** – Clears all filter settings (as described above).
- **Copy/Copy all** – Copies information about all the records in the window.
- **Delete/Delete all** – Deletes the selected record(s) or all the records displayed – this action requires administrator privileges.
- **Export...** – Exports information about the record(s) in XML format.
- **Export all...** – Export information about all records in XML format.
- **Scroll log** – Leave this option enabled to auto scroll old logs and view active logs in the **Log files** window.

4.4.1.1.1 Log files

The Logging configuration of ESET NOD32 Antivirus is accessible from the main program window. Click **Setup** > **Enter advanced setup...** > **Tools** > **Log files**. The logs section is used to define how the logs will be managed. The program automatically deletes older logs in order to save hard disk space. You can specify the following options for log files:

Minimum logging verbosity – Specifies the minimum verbosity level of events to be logged.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as *"Error downloading file"* and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting Antivirus protection, etc...).

Log entries older than the specified number of days in the **Automatically delete records older than (days)** field will automatically be deleted.

Optimize log files automatically – If checked, log files will be automatically be defragmented if the percentage is higher than value specified in the **If the number of unused records exceeds (%)** field.

Click **Optimize** to begin defragmenting the log files. All empty log entries are removed during this process, which improves performance and log processing speed. This improvement can be observed especially if the logs contain a large number of entries.

Enable text protocol enables the storage of logs in another file format separate from Log files:

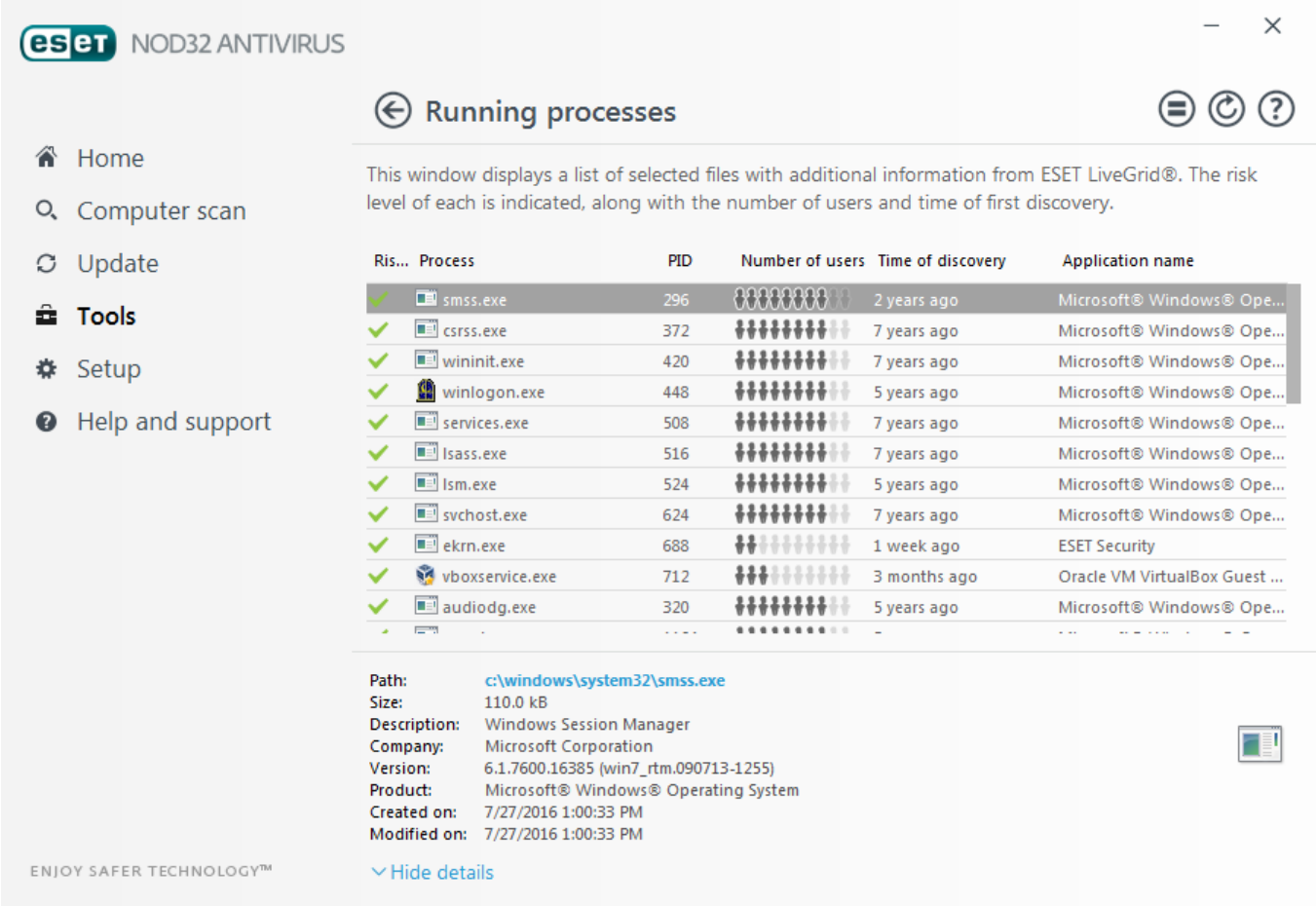
- **Target directory** – The directory where log files will be stored (only applies to Text/CSV). Each log section has its own file with a predefined file name (for example, *virlog.txt* for the **Detected threats** section of log files, if you use a plain text file format to store logs).
- **Type** – If you select the **Text** file format, logs will be stored in a text file and data will be separated into tabs. The same applies to the comma-separated **CSV** file format. If you choose **Event**, logs will be stored in the Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to the file.

Delete all logs files – Erases all stored logs currently selected in the **Type** drop-down menu. A notification about successful deletion of the logs will be shown.

NOTE
In order to help resolve issues more quickly, ESET may ask you to provide logs from your computer. ESET Log Collector makes it easy for you to collect the information needed. For more information about ESET Log Collector please visit our ESET Knowledgebase article.

4.4.1.2 Running processes

Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET NOD32 Antivirus provides detailed information on running processes to protect users with ThreatSense technology.


NOD32 ANTIVIRUS
Running processes
Home
Computer scan
Update
Tools
Setup
Help and support
This window displays a list of selected files with additional information from ESET LiveGrid®. The risk level of each is indicated, along with the number of users and time of first discovery.
Ris... Process PID Number of users Time of discovery Application name
smss.exe 296 2 years ago Microsoft® Windows® Ope...
csrss.exe 372 7 years ago Microsoft® Windows® Ope...
wininit.exe 420 7 years ago Microsoft® Windows® Ope...
winlogon.exe 448 5 years ago Microsoft® Windows® Ope...
services.exe 508 7 years ago Microsoft® Windows® Ope...
lsass.exe 516 7 years ago Microsoft® Windows® Ope...
lsm.exe 524 5 years ago Microsoft® Windows® Ope...
svchost.exe 624 7 years ago Microsoft® Windows® Ope...
ekrn.exe 688 1 week ago ESET Security
vboxservice.exe 712 3 months ago Oracle VM VirtualBox Guest ...
audiodg.exe 320 5 years ago Microsoft® Windows® Ope...
Path: c:\windows\system32\smss.exe
Size: 110.0 kB
Description: Windows Session Manager
Company: Microsoft Corporation
Version: 6.1.7600.16385 (win7_rtm.090713-1255)
Product: Microsoft® Windows® Operating System
Created on: 7/27/2016 1:00:33 PM
Modified on: 7/27/2016 1:00:33 PM
Hide details
ENJOY SAFER TECHNOLOGY™

Process – Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. To open Task Manager, right-click an empty area on the taskbar and then click **Task Manager**, or press **Ctrl**+**Shift**+**Esc** on your keyboard.

Risk level – In most cases, ESET NOD32 Antivirus and ThreatSense technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 – Fine (green) to 9 – Risky (red).

NOTE
Known applications marked as Fine (green) are definitely clean (whitelisted) and will be excluded from scanning to improve performance.

PID – The process identifier number may be used as a parameter in various function calls such as adjusting the process's priority.

Number of users – The number of users that use a given application. This information is gathered by ThreatSense technology.

Time of discovery – Period of time since the application was discovered by ThreatSense technology.

NOTE
An application marked as Unknown (orange) is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, you can submit the file for analysis to the ESET Research Lab. If the file turns out to be a malicious application, its detection will be added to an upcoming update.

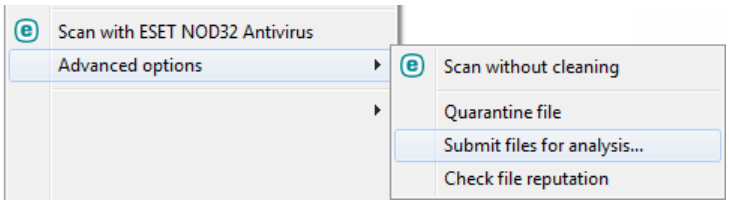
Application name – The given name of a program or process.

Open in a new window – The running processes information will be opened in a new window.

Click an application to display the following details of that application:

- **Path** – Location of an application on your computer.
- **Size** – File size in B (bytes).
- **Description** – File characteristics based on the description from the operating system.
- **Company** – Name of the vendor or application process.
- **Version** – Information from the application publisher.
- **Product** – Application name and/or business name.
- **Created on/Modified on** – Date and time of creation (modification).

NOTE
You can also check the reputation of files that do not act as running programs/processes. To do so, right-click them and select **Advanced options** > **Check file reputation**.



4.4.1.3 Protection statistics

To view a graph of statistical data related to ESET NOD32 Antivirus's protection modules, click **Tools** > **Protection statistics**. Select the desired protection module from the **Statistics** drop-down menu to see the corresponding graph and legend. If you mouse over an item in the legend, only the data for that item will display in the graph.

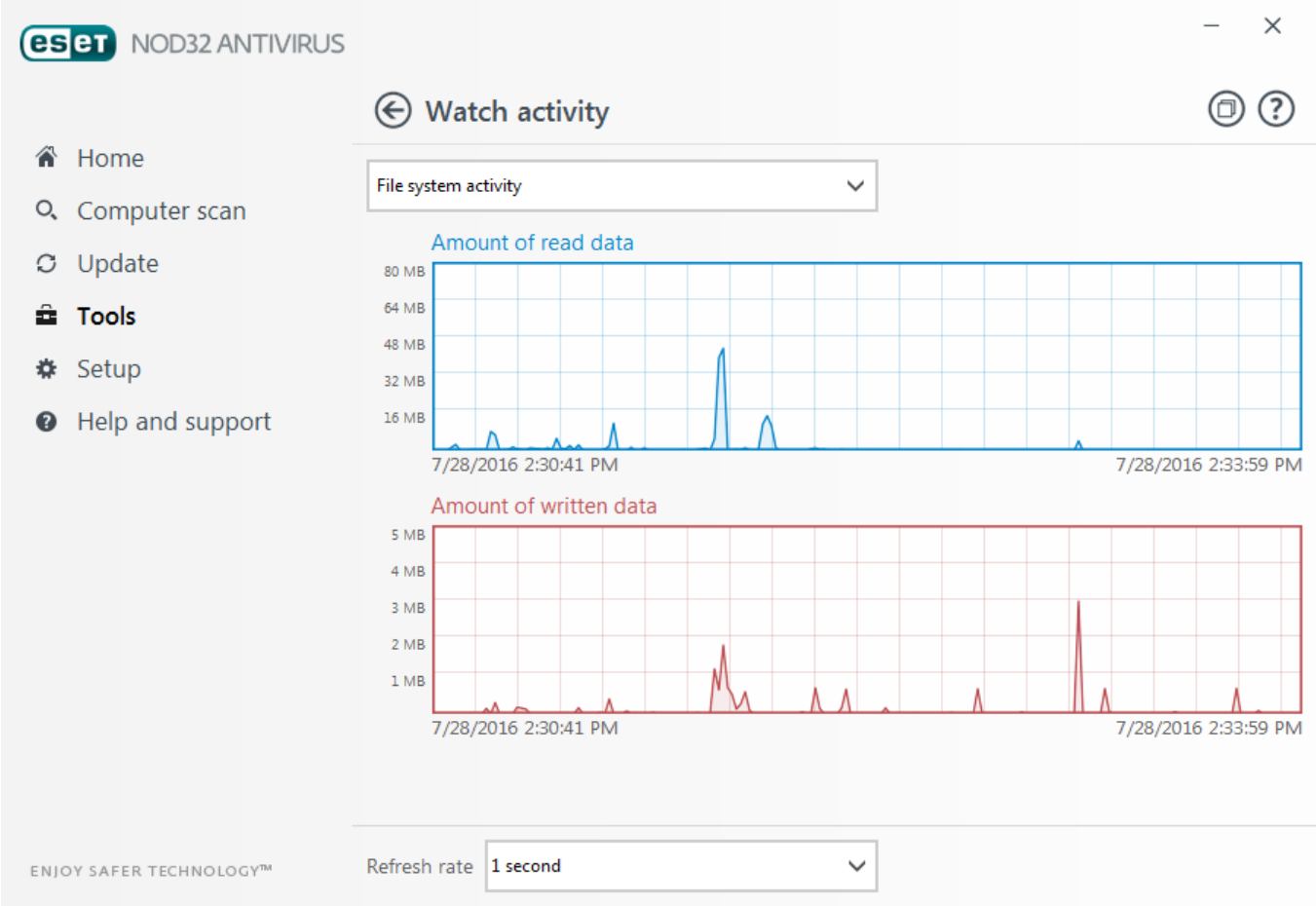
The following statistic graphs are available:

- **Antivirus and Antispyware protection** – Displays the number of infected and cleaned objects.
- **File system protection** – Only displays objects that were read or written to the file system.
- **Email client protection** – Only displays objects that were sent or received by email clients.
- **Web access and Anti-Phishing protection** – Only displays objects downloaded by web browsers.

Below the statistics graphs, you can see the number of total scanned objects, latest scanned object and the statistics timestamp. Click **Reset** to clear all statistics information.

4.4.1.4 Watch activity

To see the current **File system activity** in graph form, click **Tools** > **Watch activity**. At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. To change the time span, select from **Refresh rate** drop-down menu.



The following options are available:

- **Step: 1 second** – The graph refreshes every second and the timeline covers the last 10 minutes.
- **Step: 1 minute (last 24 hours)** – The graph is refreshed every minute and the timeline covers the last 24 hours.
- **Step: 1 hour (last month)** – The graph is refreshed every hour and the timeline covers the last month.
- **Step: 1 hour (selected month)** – The graph is refreshed every hour and the timeline covers the last X selected months.

The vertical axis of the **File system activity graph** represents read data (blue) and written data (red). Both values are given in KB (kilobytes)/MB/GB. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

4.4.1.5 ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components such as drivers and applications, network connections or important registry entries and assesses the risk level of each component. This information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection.

The SysInspector window displays the following information about created logs:

- **Time** – The time of log creation.
- **Comment** – A short comment.
- **User** – The name of the user who created the log.
- **Status** – The status of log creation.

The following actions are available:

- **Show** – Opens created log. You can also right-click a given log file and select **Show** from the context menu.
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **Delete** – Removes the selected log(s) from the list.

The following items are available from the context menu when one or more log files are selected:

- **Show** – Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **Delete** – Removes the selected log(s) from the list.
- **Delete all** – Deletes all logs.
- **Export...** – Exports the log to an *.xml* file or zipped *.xml*.

4.4.1.6 Scheduler

Scheduler manages and launches scheduled tasks with predefined configuration and properties.

The Scheduler can be accessed from the ESET NOD32 Antivirus main program window by clicking **Tools** > **Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time and scanning profile used.

The Scheduler serves to schedule the following tasks: virus signature database update, scanning task, system startup file check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add...** or **Delete** at the bottom). Right click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, and delete an existing task. Use the checkboxes at the beginning of each entry to activate/deactivate the tasks.

By default, the following scheduled tasks are displayed in **Scheduler**:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Regular checking for latest product version** (see Update mode)
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit...** or select the task you want to modify and click **Edit...**.

Add a new task

1. Click **Add task** at the bottom of the window.
2. Enter a name of the task.

3. Select the desired task from the pull-down menu:

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer scan** – Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** – Performs a computer scan of files and folders on your computer.
- **Update** – Schedules an Update task by updating the virus signature database and program modules.

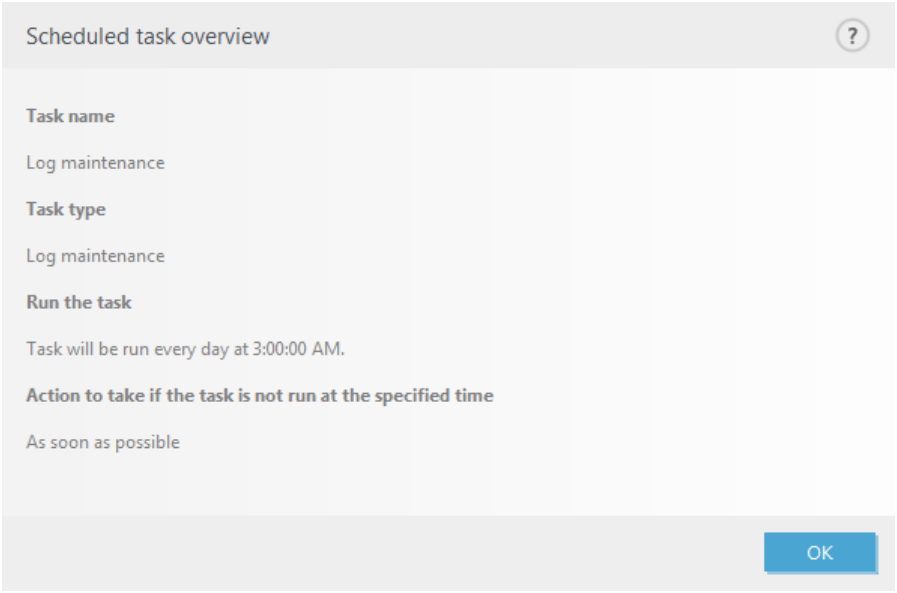
4. Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting checkbox in the list of scheduled tasks), click **Next** and select one of the timing options:

- **Once** – The task will be performed at the predefined date and time.
- **Repeatedly** – The task will be performed at the specified time interval.
- **Daily** – The task will run repeatedly each day at the specified time.
- **Weekly** – The task will be run on the selected day and time.
- **Event triggered** – The task will be performed on a specified event.

5. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. If the task could not be run at the predefined time, you can specify when it will be performed again:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if the time since the last run exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

You can review scheduled task when right click and click **Show task details**.


Scheduled task overview
Task name
Log maintenance
Task type
Log maintenance
Run the task
Task will be run every day at 3:00:00 AM.
Action to take if the task is not run at the specified time
As soon as possible
OK

4.4.1.7 ESET SysRescue

ESET SysRescue is a utility that enables you to create a bootable disk containing one of the ESET Security solutions - ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium or certain server-oriented products. The main advantage of ESET SysRescue is the fact that the ESET Security solution runs independent of the host operating system but has direct access to the disk and file system. This makes it possible to remove infiltrations which normally could not be deleted, for example, when the operating system is running, etc.

4.4.1.8 ESET LiveGrid®

ESET LiveGrid® (built on the ESET ThreatSense.Net advanced early warning system) utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to needs of our customers and keep ESET responsive to the latest threats. Read more about ESET LiveGrid® in the glossary.

A user can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®. There are two options:

1. You can choose not to enable ESET LiveGrid®. You will not lose any functionality in the software, but in some cases, ESET NOD32 Antivirus may respond faster to new threats than virus signature database update when ESET Live Grid is enabled.
2. You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

ESET LiveGrid® will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer's operating system.

By default, ESET NOD32 Antivirus is configured to submit suspicious files to the ESET Virus Lab for detailed analysis. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are particular files that you or your organization wants to avoid sending.

The ESET LiveGrid® setup menu provides several options for enabling / disabling ESET LiveGrid®, which serves to submit suspicious files and anonymous statistical information to ESET labs. It is accessible from the Advanced setup tree by clicking **Tools** > **ESET LiveGrid®**.

Enable ESET LiveGrid® reputation system (recommended) – The ESET LiveGrid® reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

Submit anonymous statistics – Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, product version, and configuration including information about your system.

Submit files – Suspicious files resembling threats, and/or files with unusual characteristics or behavior are submitted to ESET for analysis.

Select **Enable logging** to create an event log to record file and statistical information submissions. This will enable logging to the Event log when files or statistics are sent.

Contact email (optional) – Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

Exclusion – The Exclusion filter allows you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

If you have used ESET LiveGrid® before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. Once all current information is sent, no further packages will be created.

4.4.1.8.1 Suspicious files

If you find a suspicious file, you can submit it for analysis to our ESET Research Lab. If it is a malicious application, its detection will be added to the next virus signature update.

Exclusion filter – The Exclusion filter allows you to exclude certain files/folders from submission. The files listed will never be sent to ESET Research Lab for analysis, even if they contain a suspicious code. For example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

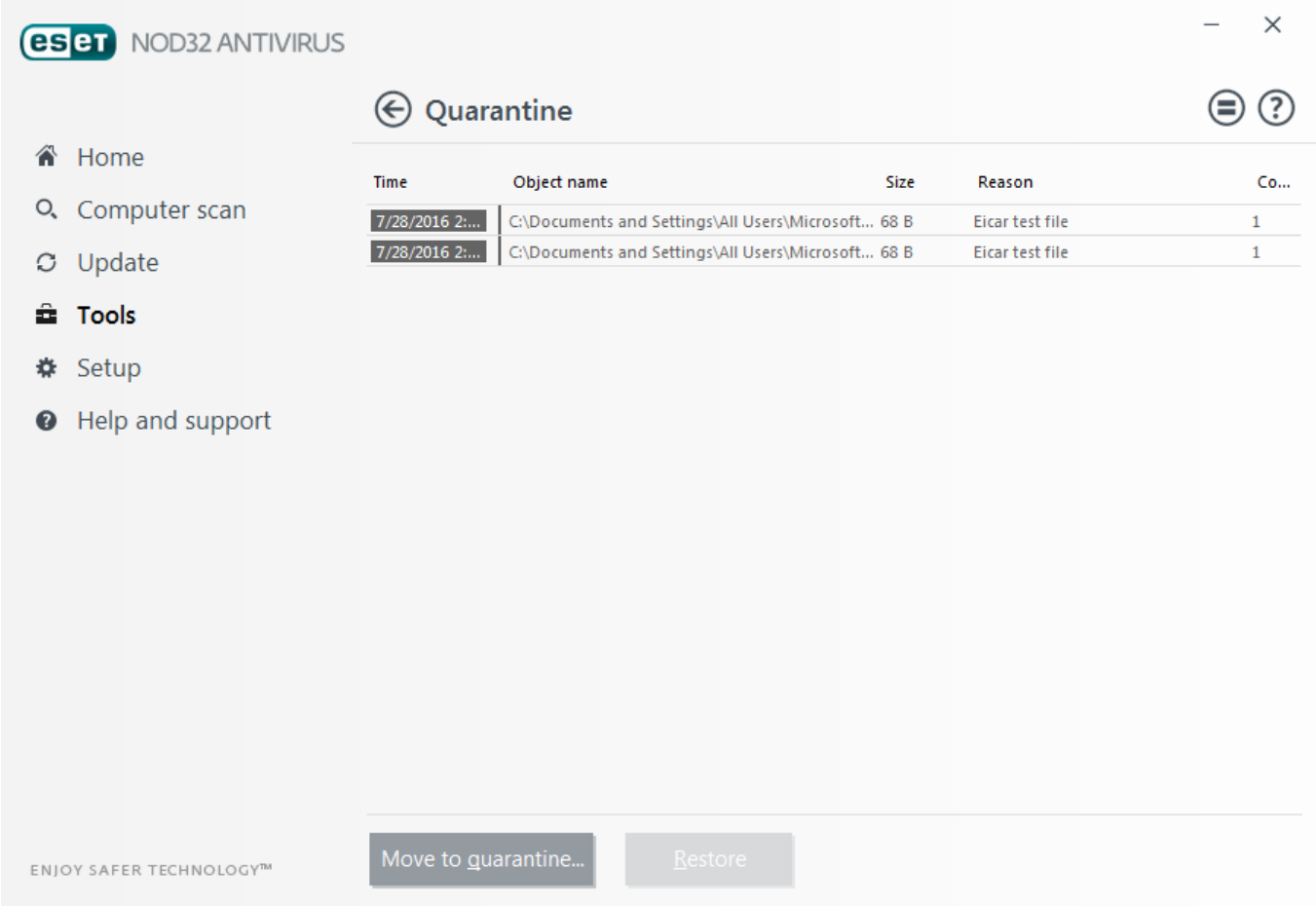
Contact email (optional) – Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

Select **Enable logging** to create an event log to record file and statistical information submissions. This will enable logging to the Event log when files or statistics are sent.

4.4.1.9 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET NOD32 Antivirus.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Research Lab.



Files stored in the quarantine folder can be viewed in a table that displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (for example, object added by user), and number of threats (for example, if it is an archive containing multiple infiltrations).

Quarantining files

ESET NOD32 Antivirus automatically quarantines deleted files (if you have not canceled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Quarantine...**. If this is the case, the

original file will not be removed from its original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine...**.

Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature for this purpose, which is available from the context menu by right-clicking a given file in the Quarantine window. If a file is marked as potentially unwanted application, the **Restore and exclude from scanning** option is enabled. Read more about this type of application in the glossary. The context menu also offers the **Restore to...** option which allows you to restore a file to a location other than the one from which it was deleted.

NOTE
If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

4.4.1.10 Proxy server

In large LAN networks, communication between your computer and the internet can be mediated by a proxy server. Using this configuration, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET NOD32 Antivirus, proxy server setup is available from two different sections of the Advanced setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET NOD32 Antivirus. Parameters here will be used by all modules that require a connection to the Internet.

To specify proxy server settings for this level, select **Use proxy server** and enter the address of the proxy server into the **Proxy server** field along with the **Port** number of the proxy server.

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and enter a valid **Username** and **Password** into the respective fields. Click **Detect** to automatically detect and populate proxy server settings. The parameters specified in Internet Explorer will be copied.

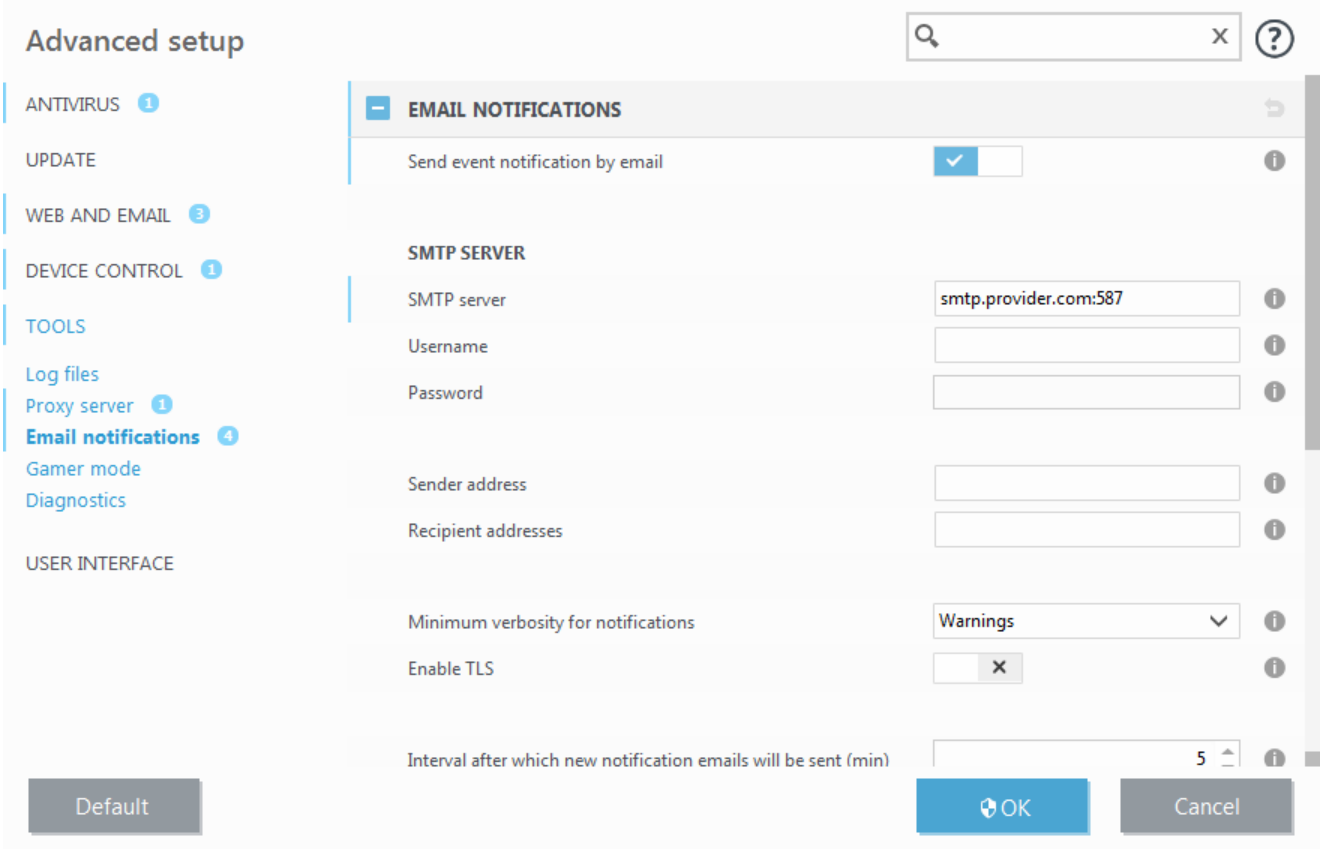
NOTE
You must manually enter your Username and Password in **Proxy server** settings.

Use direct connection if proxy is not available – If a product is configured to utilize HTTP Proxy and the proxy is unreachable, the product will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be established from Advanced update setup (**Advanced setup** > **Update** > **HTTP Proxy** by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu). This setting applies for the given update profile and is recommended for laptops that often receive virus signature updates from remote locations. For more information about this setting, see Advanced update setup.

4.4.1.11 Email notifications

ESET NOD32 Antivirus can automatically send notification emails if an event with the selected verbosity level occurs. Enable **Send event notifications by email** to activate email notifications.



SMTP server

SMTP server – The SMTP server used for sending notifications (e.g. *smtp.provider.com:587*, predefined port is 25).

> **NOTE**
> SMTP servers with TLS encryption are supported by ESET NOD32 Antivirus.

Username and **password** – If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.

Sender address – This field specifies the sender address that will be displayed in the header of notification emails.

Recipient address – This field specifies the recipient address that will be displayed in the header of notification emails.

From the **Minimum verbosity for notifications** drop-down menu, you can select the starting severity level of notifications to be sent.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages (Antistealth is not running properly or update failed).
- **Errors** – Errors (document protection not started) and critical errors will be recorded.
- **Critical** – Logs only critical errors error starting antivirus protection or infected system.

Enable TLS – Enable sending alert and notification messages supported by TLS encryption.

Interval after which new notification emails will be sent (min) – Interval in minutes after which new notifications will be sent to email. If you set this value to 0, the notifications will be sent immediately.

Sent each notification in a separate email – When enabled, the recipient will receive a new email for each individual notification. This may result in large number of emails being received in a short period of time.

Message format

Format of event messages – Format of event messages that are displayed on remote computers.

Format of threat warning messages – Threat alert and notification messages have a predefined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Use local alphabetic characters – Converts an email message to the ANSI character encoding based upon Windows Regional settings (for example, windows-1250). If you leave this deselected, a message will be converted and encoded in ACSII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?").

Use local character encoding – The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

4.4.1.11.1 Message format

Here you can set up the format of event messages that are displayed on remote computers.

Threat alert and notification messages have a predefined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Keywords (strings separated by % signs) are replaced in the message by the actual information as specified. The following keywords are available:

- **%TimeStamp%** – Date and time of the event
- **%Scanner%** – Module concerned
- **%ComputerName%** – Name of the computer where the alert occurred
- **%ProgramName%** – Program that generated the alert
- **%InfectedObject%** – Name of infected file, message, etc
- **%VirusName%** – Identification of the infection
- **%ErrorDescription%** – Description of a non-virus event

The keywords **%InfectedObject%** and **%VirusName%** are only used in threat warning messages, and **%ErrorDescription%** is only used in event messages.

Use local alphabetic characters – Converts an email message to the ANSI character encoding based upon Windows Regional settings (e.g. windows-1250). If you leave this deselected, a message will be converted and encoded in ACSII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?").

Use local character encoding – The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

4.4.1.12 Select sample for analysis

The file submission dialog enables you to send a file or a site to ESET for analysis and can be found in **Tools** > **Submit sample for analysis**. If you find a suspiciously behaving file on your computer or suspicious site on the Internet, you can submit it to the ESET Research Lab for analysis. If the file turns out to be a malicious application or website, its detection will be added to an upcoming update.

Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).

NOTE
Before submitting a file to ESET, make sure it meets one or more of the following criteria:

- the file is not detected at all
- the file is incorrectly detected as a threat

You will not receive a response unless further information is required for analysis.

Select the description from the **Reason for submitting the file** drop-down menu that best fits your message:
- **Suspicious file**
- **Suspicious site** (a website that is infected by any malware),
- **False positive file** (file that is detected as an infection but are not infected),
- **False positive site**
- **Other**

File/Site – The path to the file or website you intend to submit.

Contact email – This contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional. The sample can be **submitted anonymously**. You will not get a response from ESET unless more information is required, since each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.

4.4.1.13 Microsoft Windows® update

The Windows update feature is an important component of protecting users from malicious software. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET NOD32 Antivirus notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** – No system updates will be offered for download.
- **Optional updates** – Updates marked as low priority and higher will be offered for download.
- **Recommended updates** – Updates marked as common and higher will be offered for download.
- **Important updates** – Updates marked as important and higher will be offered for download.
- **Critical updates** – Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Accordingly, the system update information may not be immediately available after saving changes.

4.5 User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI).

Using the Graphics tool, you can adjust the program's visual appearance and effects used.

By configuring Alerts and notifications, you can change the behavior of detected threat alerts and system notifications. These can be customized to fit your needs.

To provide maximum security of your security software, you can prevent any unauthorized changes by protecting the settings by a password using the Access setup tool.

4.5.1 User interface elements

User interface configuration options in ESET NOD32 Antivirus allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface** > **User interface elements** branch of the ESET NOD32 Antivirus Advanced setup tree.

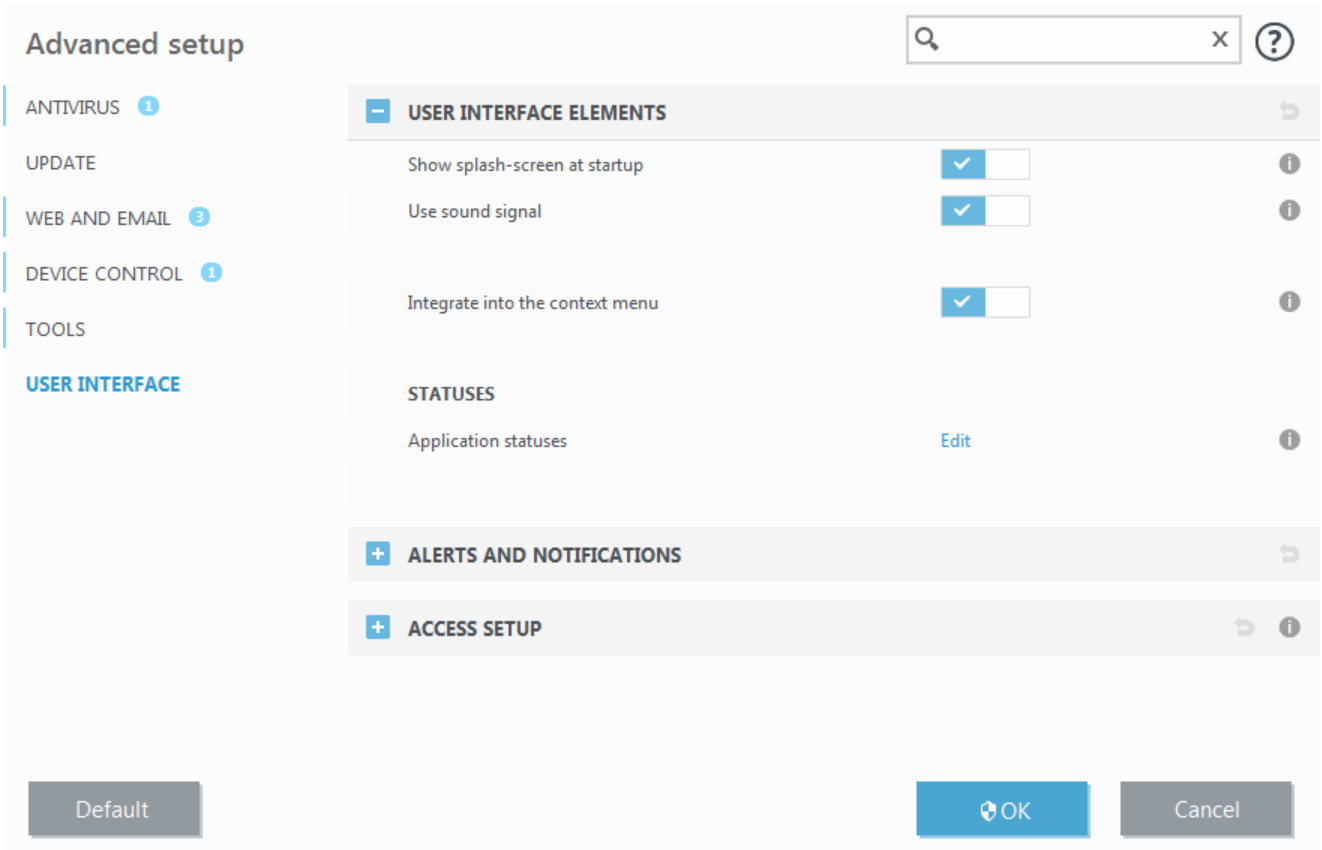
If you want to deactivate the ESET NOD32 Antivirus splash-screen, deselect **Show splash-screen at startup**.

To have ESET NOD32 Antivirus play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select **Use sound signal**.

Integrate into the context menu – Integrate the ESET NOD32 Antivirus control elements into the context menu.

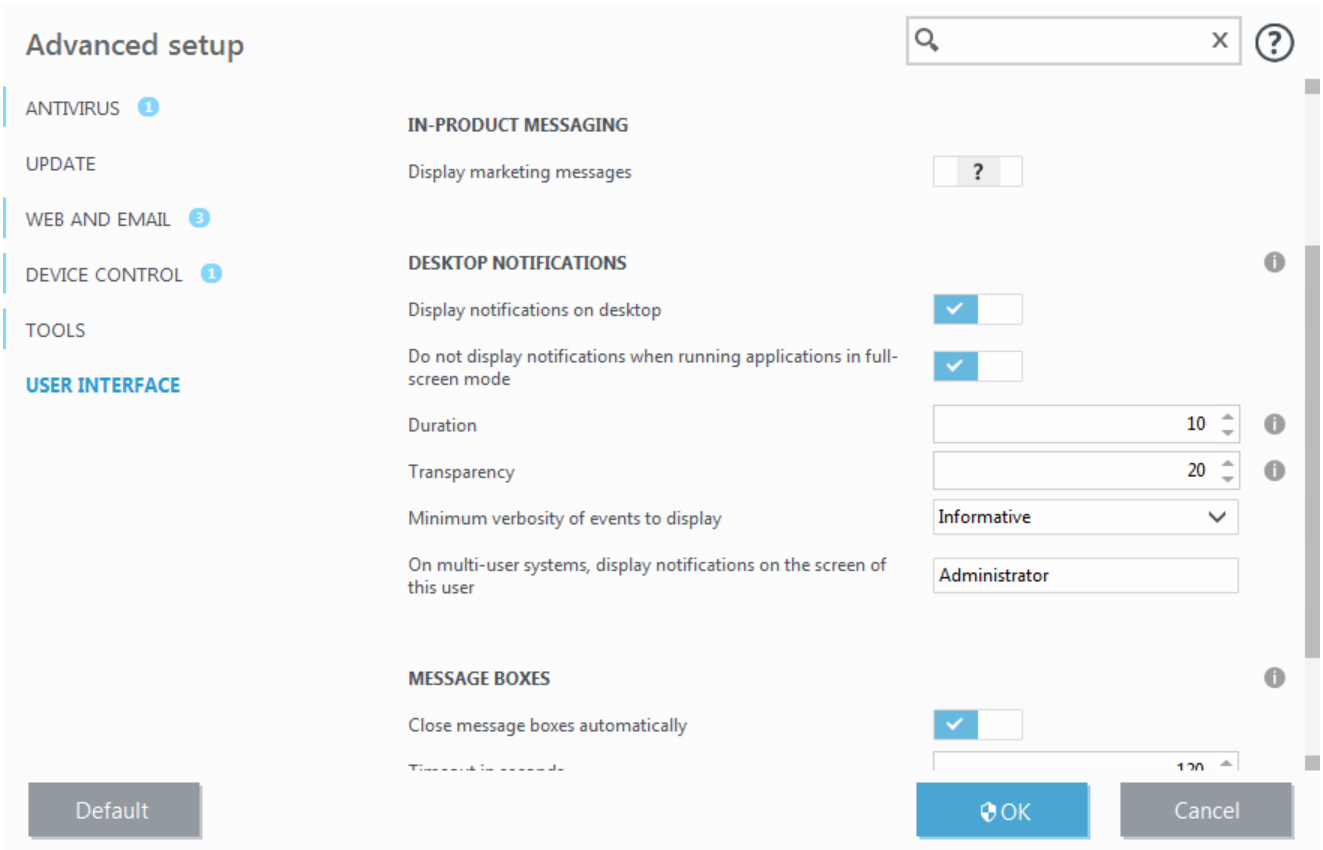
Statuses

Application statuses – Click **Edit** button to manage (disable) statuses that are displayed in the **Protection status** pane in main menu.



4.5.2 Alerts and notifications

The **Alerts and notifications** section under **User interface** allows you to configure how threat alerts and system notifications (for example, successful update messages) are handled by ESET NOD32 Antivirus. You can also set the display time and transparency of system tray notifications (this applies only on systems that support system tray notifications).



Alert windows

Disabling **Display alerts** will cancel all alert windows, and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left in its default setting (enabled).

In-product messaging

Display marketing messages – In-product messaging has been designed to inform users of ESET news and other communications. Disable this option if you do not want to receive marketing messages.

Desktop notifications

Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select **Display notifications on desktop**.

Enable **Do not display notifications when running applications in full-screen mode** to suppress all non-interactive notifications. More detailed options, such as notification display time and window transparency can be modified below.

The **Minimum verbosity of events to display** drop-down menu allows you to select the severity level of alerts and notifications to be displayed. The following options are available:

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting antivirus protection, etc...).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies which user will receive system and other notifications on systems allowing multiple users to connect at the same time. Normally, this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

Message boxes

To close pop-up windows automatically after a certain period of time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time period elapses.

Confirmation messages – Shows you a list of confirmation messages that you can select to display or not to display.

4.5.2.1 Advanced setup

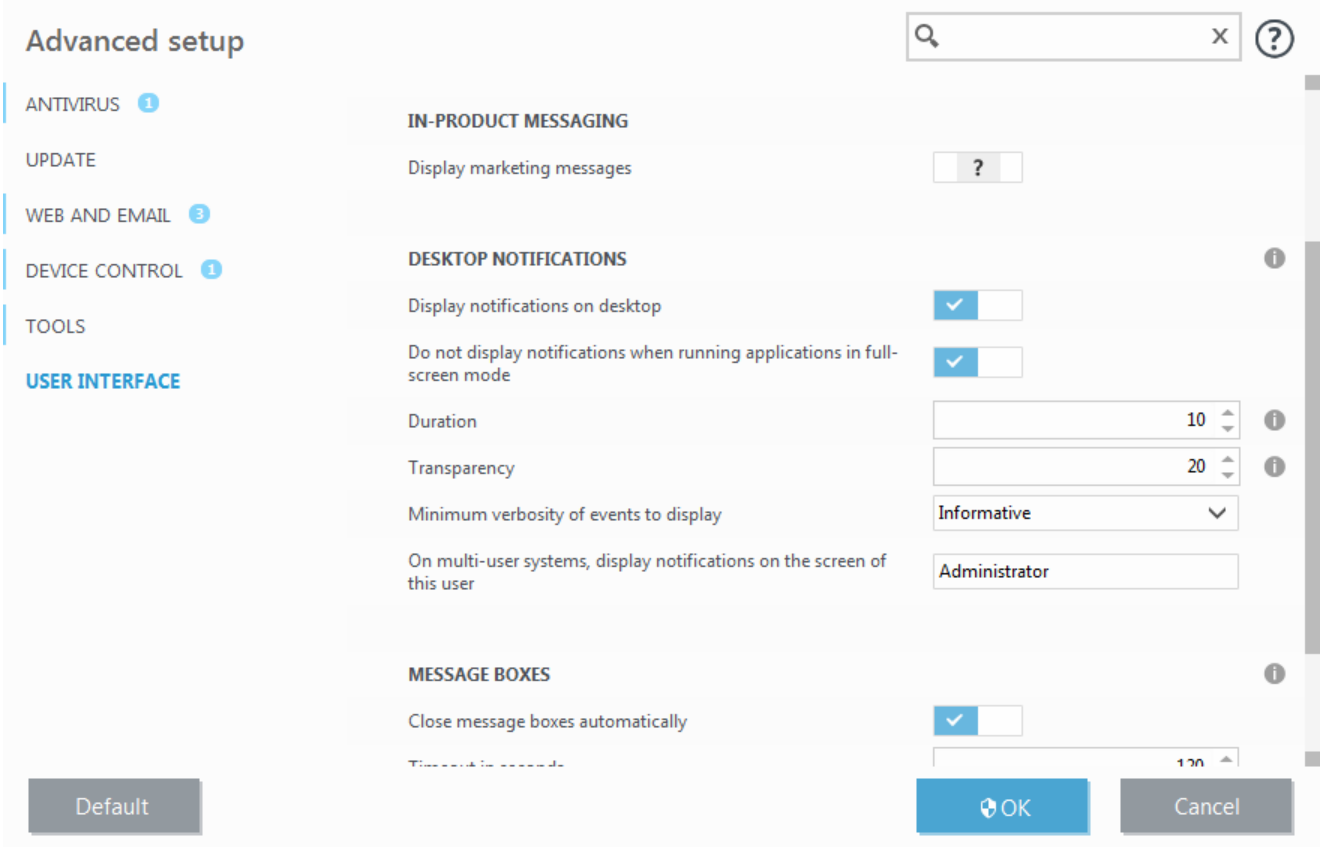
From the **Minimum verbosity of events to display** drop-down menu, you can select the starting severity level of alerts and notification to be displayed.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as *"Error downloading file"* and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting Antivirus protection, etc...).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies a user who will receive system and other notifications on systems allowing multiple users to connect at the same time. Normally, this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

4.5.3 Access setup

ESET NOD32 Antivirus settings are a crucial part of your security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To avoid unauthorized modifications, the setup parameters of ESET NOD32 Antivirus can be password protected.



Password protect settings – Indicate password settings. Click to open the Password setup window.

To set or change a password to protect setup parameters, click **Set**.

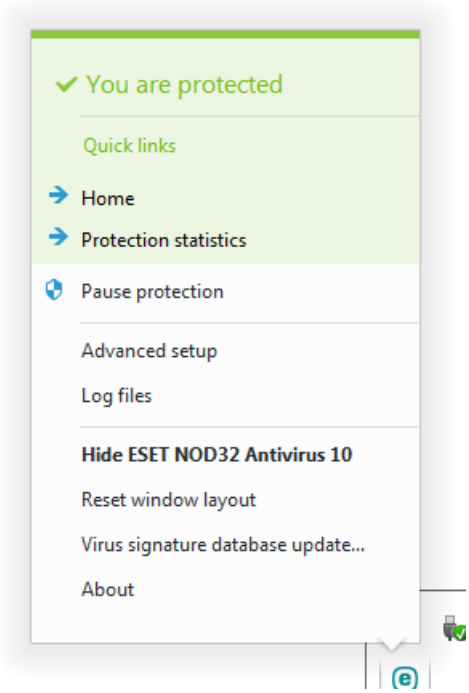
Require full administrator rights for limited administrator accounts – Select this to prompt the current user (if he or she does not have administrator rights) to enter an administrator username and password when modifying certain system parameters (similar to the User Account Control (UAC) in Windows Vista and Windows 7). Such modifications include disabling protection modules. On Windows XP systems where UAC is not running, users will have the **Require administrator rights (system without UAC support)** option available.

For Windows XP only:

Require administrator rights (system without UAC support) – Enable this option to have ESET NOD32 Antivirus prompt for administrator credentials.

4.5.4 Program menu

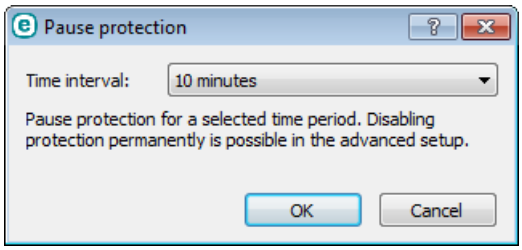
Some of the most important setup options and features are available by right-clicking the system tray icon .



Quick links – Displays the most frequently used parts of ESET NOD32 Antivirus. You can quickly access these from the program menu.

Pause protection – Displays the confirmation dialog box that disables Antivirus and antispyware protection, which guards against malicious system attacks by controlling file, web and email communication.

The **Time interval** drop-down menu represents the period of time that Antivirus and antispyware protection will be disabled for.


Pause protection
Time interval:
10 minutes
Pause protection for a selected time period. Disabling protection permanently is possible in the advanced setup.
OK
Cancel

Advanced setup – Select this option to enter the **Advanced setup** tree. There are also other ways to open Advanced setup, such as pressing the F5 key or navigating to **Setup** > **Advanced setup**.

Log files – Log files contain information about important program events that have occurred and provide an overview of detected threats.

Hide ESET NOD32 Antivirus – Hide the ESET NOD32 Antivirus window from the screen.

Reset window layout – Resets the ESET NOD32 Antivirus's window to its default size and position on the screen.

Virus signature database update – Starts updating the virus signature database to ensure your level of protection against malicious code.

About – Provides system information, details about the installed version of ESET NOD32 Antivirus and the installed program modules. Here you can also find the license expiration date and information about the operating system and system resources.

5. Advanced user

5.1 Profile manager

Profile manager is used in two places within ESET NOD32 Antivirus – in the **On-demand computer scan** section and in the **Update** section.

Computer scan

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced setup window (F5) and click **Antivirus** > **On-demand computer scan** > **Basic** > **List of profiles**. The **Profile manager** window includes the **Selected profile** drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

NOTE
Suppose that you want to create your own scan profile and the **Scan your computer** configuration is partially suitable, but you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. Enter the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements and click **OK** to save your new profile.

Update

The profile editor in the Update setup section allows users to create new update profiles. Create and use your own custom profiles (other than the default **My profile**) only if your computer uses multiple means to connect to update servers.

For example, a laptop that normally connects to a local server (Mirror) in the local network but downloads updates directly from ESET update servers when disconnected from the local network (business trip) might use two profiles: the first one for connecting to the local server; the other one for connecting to ESET servers. Once these profiles are configured, navigate to **Tools** > **Scheduler** and edit the update task parameters. Designate one profile as primary and the other as secondary.

Selected profile – The currently used update profile. To change it, choose a profile from the drop-down menu.

Add... – Create new update profiles.

The bottom part of the window lists existing profiles.

5.2 Keyboard shortcuts

For better navigation in your ESET product, the following keyboard shortcuts can be used:

F1	opens help pages
F5	opens Advanced setup
Up/Down	navigation in product through items
-	collapses Advanced setup tree nodes
TAB	moves the cursor in a window
Esc	closes the active dialog window

5.3 Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, *ekrn*). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET NOD32 Antivirus problems. Click the drop-down menu next to **Dump type** and select one of three available options:

- Select **Disable** (default) to disable this feature.
- **Mini** – Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited, however because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- **Full** – Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

Enable Protocol filtering advanced logging – Record all data passing through Protocol filtering engine in PCAP format in order to help developers diagnose and fix the problems related to Protocol filtering.

Log files can be found in:
C:\ProgramData\ESET\ESET NOD32 Antivirus\Diagnostics in Windows Vista and later or *C:\Documents and Settings\All Users\...* in earlier versions of Windows.

Target directory – Directory where the dump during the crash will be generated.

Open diagnostics folder – Click **Open** to open this directory in a new *Windows explorer* window.

Create diagnostic dump – Click **Create** to create diagnostic dump files in the **Target directory**.

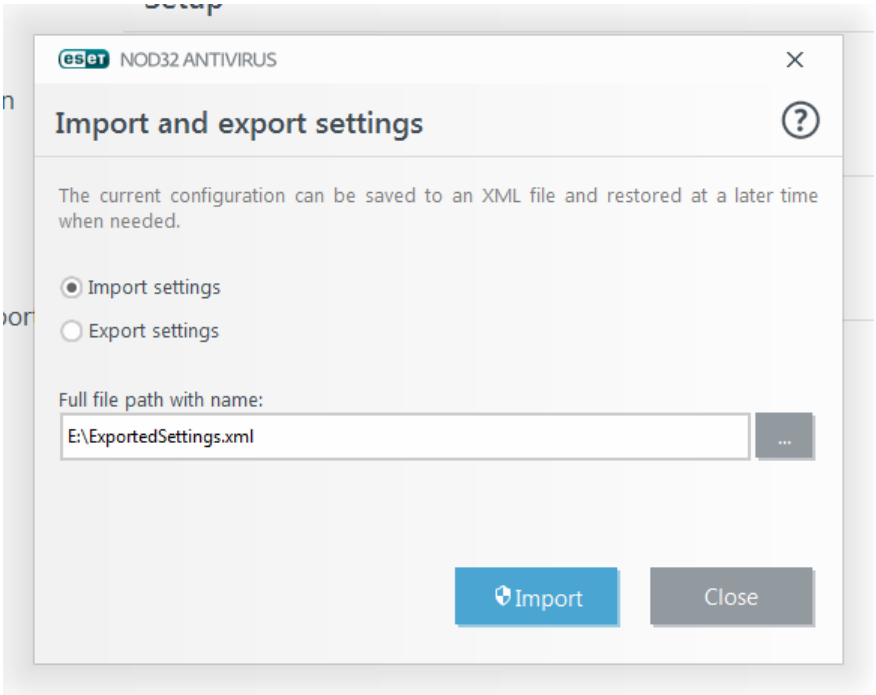
5.4 Import and export settings

You can import or export your customized ESET NOD32 Antivirus .xml configuration file from the **Setup** menu.

Importing and exporting of configuration files is useful if you need to backup your current configuration of ESET NOD32 Antivirus for use at a later time. The export settings option is also convenient for users who want to use their preferred configuration on multiple systems, they can easily import an *.xml* file to transfer these settings.

Importing a configuration is very easy. In the main program window click **Setup** > **Import and export settings**, and then select **Import settings**. Enter the file name of the configuration file or click the **...** button to browse for the configuration file you want to import.

The steps to export a configuration are very similar. In the main program window, click **Setup** > **Import and export settings**. Select **Export settings** and enter the file name of the configuration file (i.e. *export.xml*). Use the browser to select a location on your computer to save the configuration file.



NOTE
You may encounter an error while exporting settings if you do not have enough rights to write the exported file to specified directory.

5.5 ESET SysInspector

5.5.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator). For more information see section ESET SysInspector as part of ESET NOD32 Antivirus.

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

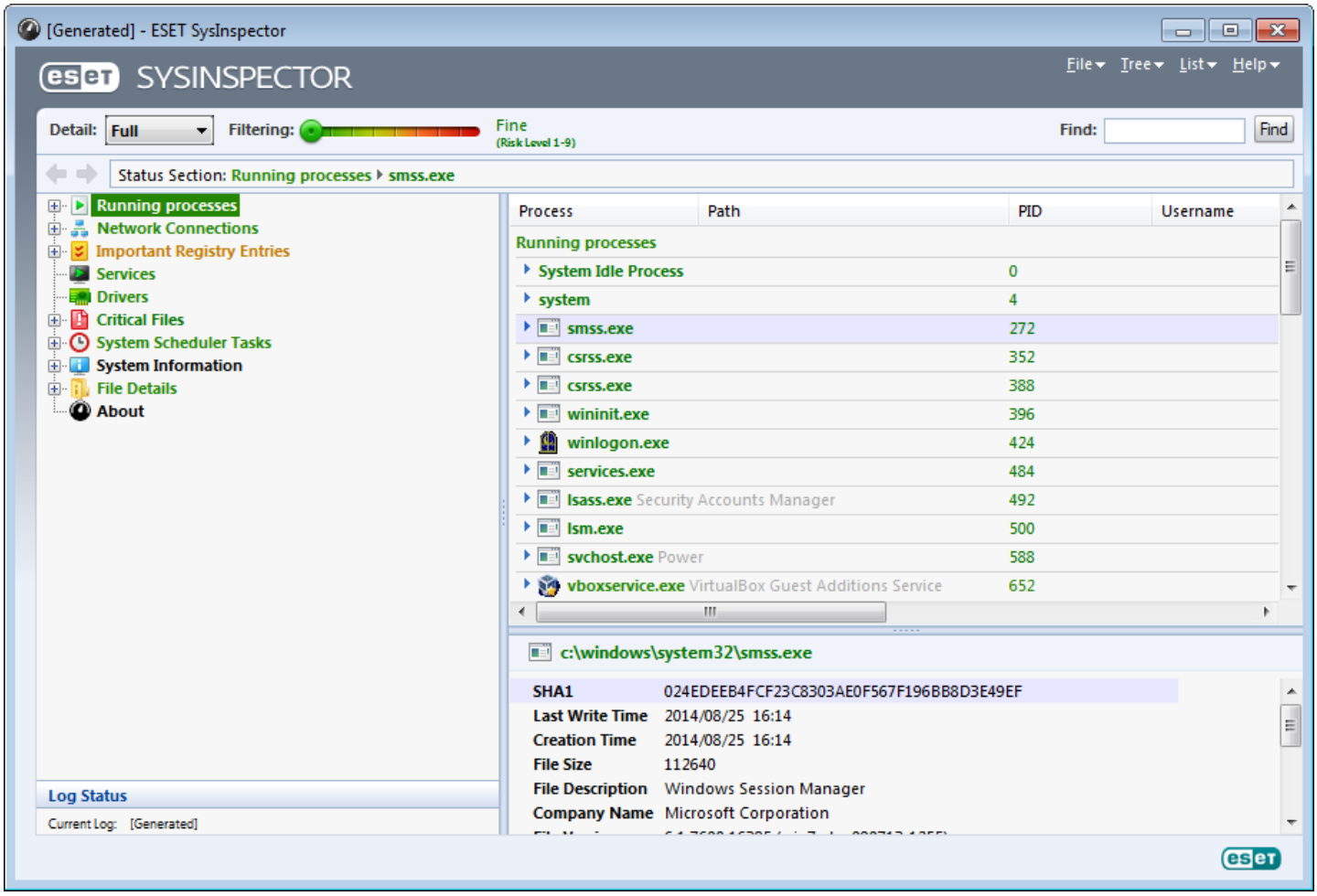
5.5.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website. If you already have one of the ESET Security solutions installed, you can run ESET SysInspector directly from the Start Menu (click **Programs** > **ESET** > **ESET NOD32 Antivirus**).

Please wait while the application inspects your system, which could take up to several minutes.

5.5.2 User Interface and application usage

For clarity the main program window is divided into four major sections – Program Controls located on the top of the main program window, Navigation window to the left, the Description window to the right and the Details window at the bottom of the main program window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



5.5.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by dragging and dropping them into the main program window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the main program window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current risk level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose a security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the **Risk Level** slider.

Compare

When comparing two logs, you can choose to display all items, display only added items, display only removed items or to display only replaced items.

Find

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return

By clicking the back or forward arrows, you can return to previously displayed information in the Description window. You can use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

5.5.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system is comprised of several important kernel components running constantly that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical files

The Description window displays content of critical files related to the Microsoft windows operating system.

System Scheduler Tasks

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

System information

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

File details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about version of ESET SysInspector and the list of program modules.

5.5.2.2.1 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O	opens existing log
Ctrl+S	saves created logs

Generate

Ctrl+G	generates a standard computer status snapshot
Ctrl+H	generates a computer status snapshot that may also log sensitive information

Item Filtering

1, O	fine, risk level 1-9 items are displayed
2	fine, risk level 2-9 items are displayed
3	fine, risk level 3-9 items are displayed
4, U	unknown, risk level 4-9 items are displayed
5	unknown, risk level 5-9 items are displayed
6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+0	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item
Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor

Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field
Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help
Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

5.5.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Click **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, click **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, click **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

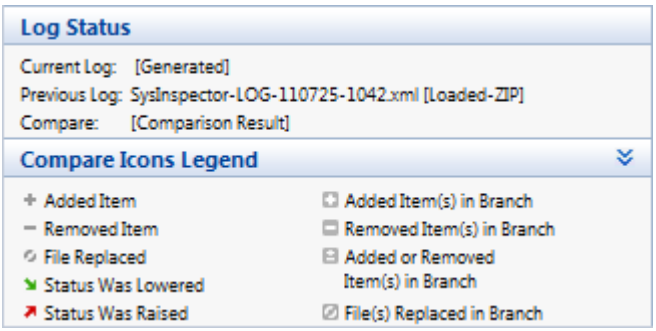
NOTE: If you compare two log files, click **File** > **Save log** to save it as a ZIP file; both files will be saved. If you open this file later, the contained logs are automatically compared.

Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- □ tree structure section contains new values
- – removed value, present in the previous log
- ⊟ tree structure section contains removed values
- ⎋ value / file has been changed
- ⊡ tree structure section contains modified values / files
- ↘ the risk level has decreased / it was higher in the previous log
- ↗ the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, click **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

SysIsnpector.exe current.xml previous.xml

5.5.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen	generate log directly from the command line without running GUI
/privacy	generate log with sensitive information omitted
/zip	save outcome log in compressed zip archive
/silent	suppress progress window when generating log from the command line
/blank	launch ESET SysInspector without generating/loading log

Examples

Usage:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

To load specific log directly into the browser, use: *SysInspector.exe .\clientlog.xml*
To generate log from the command line, use: *SysInspector.exe /gen=.\mynewlog.xml*
To generate log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
To compare two log files and browse differences, use: *SysInspector.exe new.xml old.xml*

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

5.5.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you suspect that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

1. Run ESET SysInspector to generate a new system snapshot.
2. Select the first item in the section on the left (in the tree structure), press Shift and select the last item to mark all items.
3. Right click the selected objects and select **Export Selected Sections To Service Script**.
4. The selected objects will be exported to a new log.
5. This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
6. Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
7. Click **OK** to run the script.

5.5.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either **Export All Sections To Service Script** or **Export Selected Sections To Service Script**.

NOTE: It is not possible to export the service script when two logs are being compared.

5.5.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a “+”. When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependent services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

09) Critical files

This section contains information about files that are critical to proper function of the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

10) Scheduled tasks

This section contains information about scheduled tasks.

Example:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

5.5.5 FAQ

Does ESET SysInspector require Administrator privileges to run ?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file ?

ESET SysInspector can create a log file of your computer's configuration. To save one, click **File** > **Save Log** in the main program window. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file ?

To view a log file created by ESET SysInspector, run the program and click **File** > **Open Log** in the main program window. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK ?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object ?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous ?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run ?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology ?

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time ?

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%*

*system32**catroot*) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in *C:\Program Files\Windows NT*. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* pointing to *C:\Program Files\Windows NT\hypertrm.exe* (the main executable of the HyperTerminal application) and *sp4.cat* is digitally signed by Microsoft.

5.5.6 ESET SysInspector as part of ESET NOD32 Antivirus

To open the ESET SysInspector section in ESET NOD32 Antivirus, click **Tools** > **ESET SysInspector**. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To compare, create, or delete snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, select **Show** from the context menu. To export the selected snapshot to a file, right-click it and select **Export...**.

Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.
- **Create...** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.
- **Delete/Delete all** – Removes entries from the list.
- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

5.6 Command Line

ESET NOD32 Antivirus's antivirus module can be launched via the command line – manually (with the “ecls” command) or with a batch (“bat”) file. ESET Command-line scanner usage:

```
ecls [OPTIONS..] FILES..
```

The following parameters and switches can be used while running the on-demand scanner from the command line:

Options

/base-dir=FOLDER	load modules from FOLDER
/quar-dir=FOLDER	quarantine FOLDER
/exclude=MASK	exclude files matching MASK from scanning
/subdir	scan subfolders (default)
/no-subdir	do not scan subfolders
/max-subdir-level=LEVEL	maximum sub-level of folders within folders to scan
/symlink	follow symbolic links (default)
/no-symlink	skip symbolic links
/ads	scan ADS (default)
/no-ads	do not scan ADS
/log-file=FILE	log output to FILE
/log-rewrite	overwrite output file (default – append)
/log-console	log output to console (default)
/no-log-console	do not log output to console

/log-all	also log clean files
/no-log-all	do not log clean files (default)
/aind	show activity indicator
/auto	scan and automatically clean all local disks

Scanner options

/files	scan files (default)
/no-files	do not scan files
/memory	scan memory
/boots	scan boot sectors
/no-boots	do not scan boot sectors (default)
/arch	scan archives (default)
/no-arch	do not scan archives
/max-obj-size=SIZE	only scan files smaller than SIZE megabytes (default 0 = unlimited)
/max-arch-level=LEVEL	maximum sub-level of archives within archives (nested archives) to scan
/scan-timeout=LIMIT	scan archives for LIMIT seconds at maximum
/max-arch-size=SIZE	only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited)
/max-sfx-size=SIZE	only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited)
/mail	scan email files (default)
/no-mail	do not scan email files
/mailbox	scan mailboxes (default)
/no-mailbox	do not scan mailboxes
/sfx	scan self-extracting archives (default)
/no-sfx	do not scan self-extracting archives
/rtp	scan runtime packers (default)
/no-rtp	do not scan runtime packers
/unsafe	scan for potentially unsafe applications
/no-unsafe	do not scan for potentially unsafe applications (default)
/unwanted	scan for potentially unwanted applications
/no-unwanted	do not scan for potentially unwanted applications (default)
/suspicious	scan for suspicious applications (default)
/no-suspicious	do not scan for suspicious applications
/pattern	use signatures (default)
/no-pattern	do not use signatures
/heur	enable heuristics (default)
/no-heur	disable heuristics
/adv-heur	enable Advanced heuristics (default)
/no-adv-heur	disable Advanced heuristics
/ext=EXTENSIONS	scan only EXTENSIONS delimited by colon
/ext-exclude=EXTENSIONS	exclude EXTENSIONS delimited by colon from scanning
/clean-mode=MODE	use cleaning MODE for infected objects

The following options are available:

- **none** – No automatic cleaning will occur.
- **standard** (default) – ecls.exe will attempt to automatically clean or delete infected files.
- **strict** – ecls.exe will attempt to automatically clean or delete infected files without user intervention (you will not be prompted before files are deleted).
- **rigorous** – ecls.exe will delete files without attempting to clean regardless of what the file is.
- **delete** – ecls.exe will delete files without attempting to clean, but will refrain from deleting sensitive files such as Windows system files.

/quarantine	copy infected files (if cleaned) to Quarantine (supplements the action carried out while cleaning)
/no-quarantine	do not copy infected files to Quarantine

General options

/help	show help and quit
/version	show version information and quit

/preserve-time	preserve last access timestamp

Exit codes

0	no threat found
1	threat found and cleaned
10	some files could not be scanned (may be threats)
50	threat found
100	error

NOTE
Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

6. Glossary

6.1 Types of infiltration

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

6.1.1 Viruses

A computer virus is a piece of malicious code that is pre-pended or appended to existing files on your computer. Viruses are named after biological viruses because they use similar techniques to spread from one computer to another. As for the term "virus", it is often used incorrectly to mean any type of a threat. This usage is gradually being overcome and replaced with a more accurate term "malware" (malicious software).

Computer viruses mainly attack executable files and documents. In short, this is how a computer virus works: after execution of an infected file, the malicious code is called and executed prior to the execution of the original application. A virus can infect any files that the current user has write permissions for.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

If your computer is infected with a virus and cleaning is not possible, submit it to the ESET Research Lab for perusal. In certain cases infected files can be modified to such an extent that cleaning is not possible and the files must be replaced with a clean copy.

6.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via network. The basic difference between a virus and a worm is that worms have the ability to propagate by themselves; they are not dependant on host files (or boot sectors). Worms spread to email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes after their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

6.1.3 Trojans

Historically, computer Trojans (Trojan horses) have been defined as a class of threats which attempt to present themselves as useful programs and thus trick users into running them.

Since Trojans are a very broad category, it is often divided into several subcategories:

- **Downloader** – Malicious programs with the ability to download other threats from the Internet.
- **Dropper** – Malicious programs with the ability to drop other types of malware onto compromised computers.
- **Backdoor** – Malicious programs which communicate with remote attackers, allowing them to gain access to the computer and take control over it.
- **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers.
- **Dialer** – Malicious programs designed to connect via premium-rate numbers instead of the user's Internet service provider. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

If a file on your computer is detected as a Trojan, it is advisable to delete it, since it most likely contains nothing but malicious code.

6.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1. When they try to access a system: They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2. When they are hidden from the usual testing: ESET NOD32 Antivirus users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

6.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.7 Packers

Packer is a runtime self-extracting executable that rolls up several kinds of malware into a single package.

The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

6.1.8 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET NOD32 Antivirus provides the option to detect such threats.

Potentially unsafe applications is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

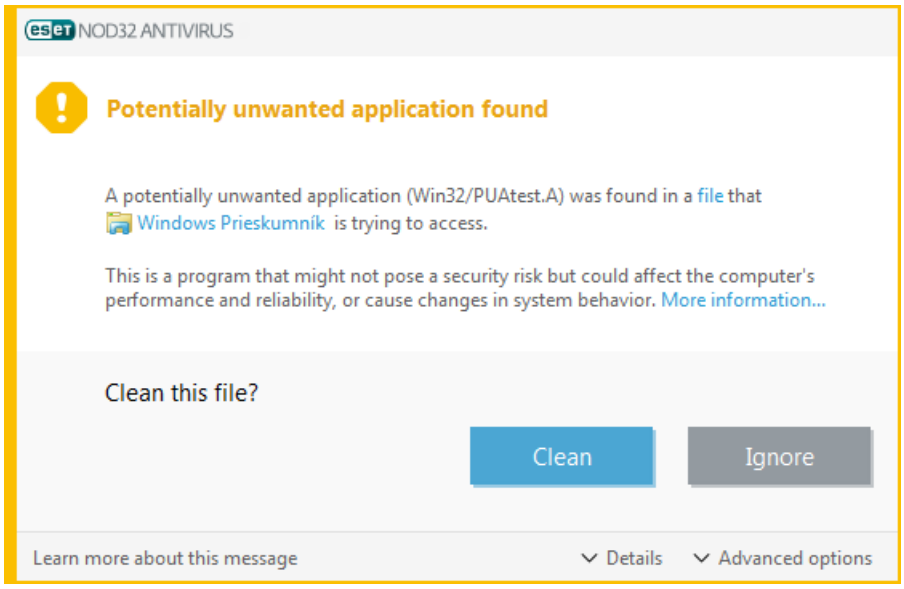
6.1.9 Potentially unwanted applications

A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives. There are some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software, such as trojan horses or worms.

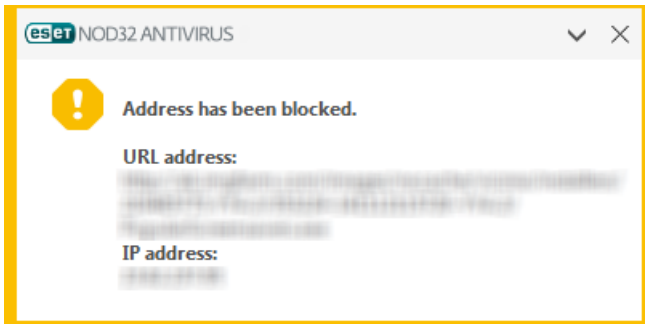
Warning - Potential threat found

When a potentially unwanted application is detected, you can decide which action to take:

1. **Clean/Disconnect**: This option ends the action and prevents the potential threat from entering your system.
2. **Ignore**: This option allows a potential threat to enter your system.
3. To allow the application to run on your computer in the future without interruption, click **Advanced options** and then select the check box next to **Exclude from detection**.

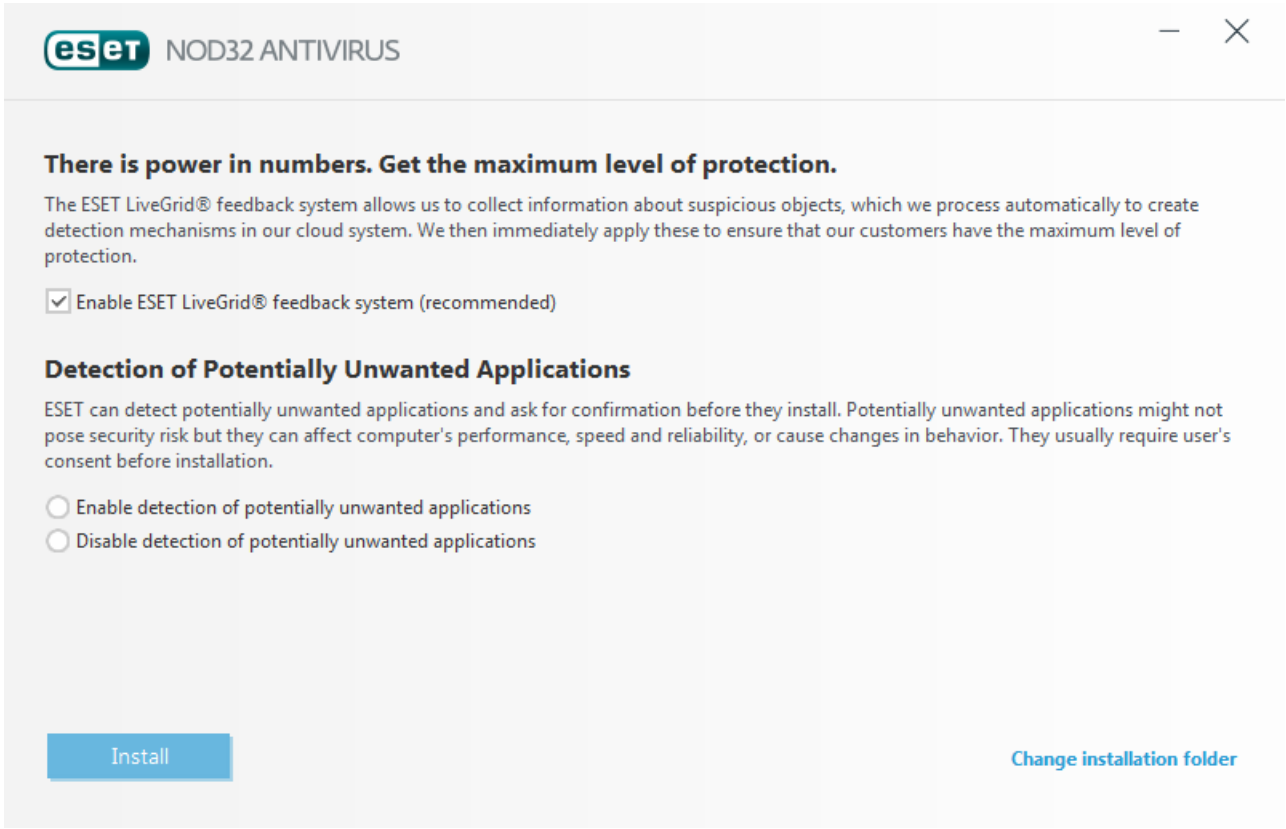

NOD32 ANTIVIRUS
Potentially unwanted application found
A potentially unwanted application (Win32/PUAtest.A) was found in a file that
Windows Prieskumník is trying to access.
This is a program that might not pose a security risk but could affect the computer's performance and reliability, or cause changes in system behavior. More information...
Clean this file?
Clean
Ignore
Learn more about this message
Details
Advanced options

When a potentially unwanted application is detected and cannot be cleaned, an **Address has been blocked** notification will be displayed. For more information about this event navigate to **Tools** > **Log files** > **Filtered websites** from the main menu.



Potentially unwanted applications - Settings

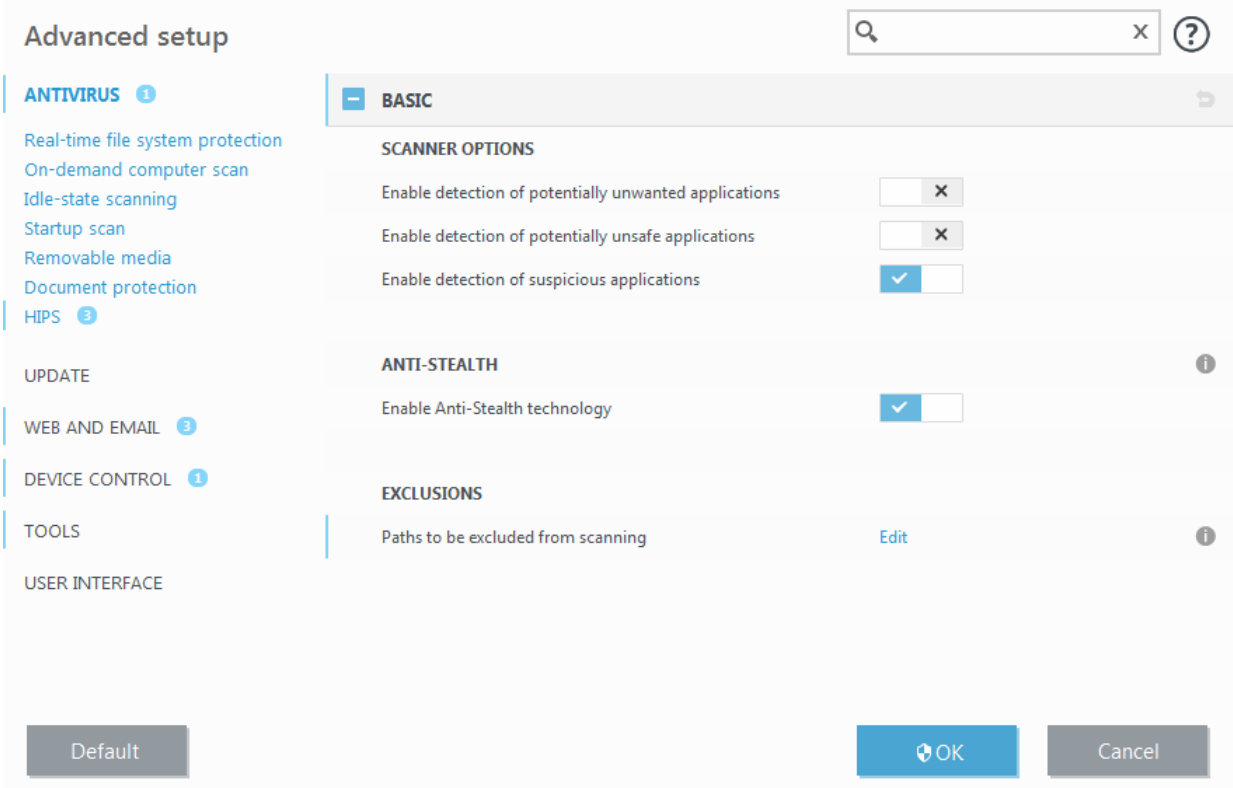
While installing your ESET product, you can decide whether to enable detection of potentially unwanted applications, as shown below:


NOD32 ANTIVIRUS
There is power in numbers. Get the maximum level of protection.
The ESET LiveGrid® feedback system allows us to collect information about suspicious objects, which we process automatically to create detection mechanisms in our cloud system. We then immediately apply these to ensure that our customers have the maximum level of protection.
Enable ESET LiveGrid® feedback system (recommended)
Detection of Potentially Unwanted Applications
ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications
Install
Change installation folder

WARNING
Potentially unwanted applications may install adware, toolbars, or contain other unwanted and unsafe program features.

These settings can be modified in your program settings at any time. To enable or disable the detection of Potentially unwanted, unsafe or suspicious applications, follow these instructions:

1. Open your ESET product. How do I open my ESET product?
2. Press the **F5** key to access **Advanced setup**.
3. Click **Antivirus** and enable or disable options **Enable detection of potentially unwanted applications**, **Enable detection of potentially unsafe applications** and **Enable detection of suspicious applications** according to your preferences. Confirm by clicking **OK**.



Potentially unwanted applications - Software wrappers

A software wrapper is a special type of application modification that is used by some file-hosting websites. It is a third-party tool that installs the program you intended to download but adds additional software, such as toolbars or adware. The additional software may also make changes to your web browser's home page and search settings. Also, file-hosting websites often do not notify the software vendor or download recipient that modifications have been made, and often hide options to opt out. For these reasons, ESET classifies software wrappers as a type of potentially unwanted application to allow users to accept the download or not.

Please see this ESET Knowledgebase article for an updated version of this help page.

6.2 ESET Technology

6.2.1 Exploit Blocker

Exploit Blocker is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. It works by monitoring the behavior of processes for suspicious activity that might indicate an exploit.

When Exploit Blocker identifies a suspicious process, it can stop the process immediately and record data about the threat, which is then sent to the ThreatSense cloud system. This data is processed by the ESET Research Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware for which there is no pre-configured remedy).

6.2.2 Advanced Memory Scanner

Advanced Memory Scanner works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation and/or encryption. In cases where ordinary emulation or heuristics might not detect a threat, the Advanced memory Scanner is able to identify suspicious behavior and scan threats when they reveal themselves in system memory. This solution is effective against even heavily obfuscated malware.

Unlike Exploit Blocker, Advanced Memory Scanner is a post-execution method, which means that there is a risk that some malicious activity could have been performed prior to its detecting a threat; however in the case that other detection techniques have failed, it offers an additional layer of security.

6.2.3 ESET LiveGrid®

Built on ThreatSense.Net® advanced early warning system, ESET LiveGrid® utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to needs of our customers and keep ESET responsive to the latest threats. ESET malware researchers use the information to build an accurate snapshot of the nature and scope of global threats, which helps us focus on the right targets. ESET LiveGrid® data plays an important role in setting priorities in our automated processing.

Additionally, it implements a reputation system that helps to improve the overall efficiency of our anti-malware solutions. When an executable file or archive is being inspected on a user's system, its hash tag is first compared against a database of white- and blacklisted items. If it is found on the whitelist, the inspected file is considered clean and also flagged to be excluded from future scans. If it is on the blacklist, appropriate actions are taken based on the nature of the threat. If no match is found, the file is scanned thoroughly. Based on the results of this scan, files are categorized as threats or non-threats. This approach has a significant positive impact on scanning performance.

This reputation system allows for effective detection of malware samples even before their signatures are delivered to user's computer via updated virus database (which happens several times a day).

6.2.4 Java Exploit Blocker

Java Exploit Blocker is an extension to existing Exploit Blocker protection. It monitors Java and looking for exploit-like behavior. Blocked samples can be reported to malware analysts, so they can create signatures to block them on different layers (URL blocking, file download, etc.).

6.2.5 Script-Based Attacks Protection

Script-Based Attacks Protection consists of protection against javascript in web browsers and Antimalware Scan Interface (AMSI) protection against scripts in Powershell.

WARNING
HIPS must be enabled for this feature to work.

Script-Based Attacks Protection supports the following web browsers:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

NOTE
The minimum supported versions of web browsers may vary because the file signature of browsers change often. The latest version of web browser is always supported.

6.2.6 Ransomware Protection

Ransomware is a type of malware that blocks users from accessing their system by locking the system's screen or by encrypting files. Ransomware protection monitors the behavior of applications and processes that try to modify your personal data. If an application's behavior is considered malicious or reputation-based scanning shows an application to be suspicious, the application is blocked or the user will be asked to block or allow it.

IMPORTANT
ESET Live Grid must be enabled for Ransomware protection to function properly.

6.3 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms – be especially cautious of options such as "Yes, I want to receive information".
- Use "specialized" email addresses – e.g., one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

6.3.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

6.3.2 Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

6.3.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

7. Common Questions

This chapter covers some of the most frequently asked questions and problems encountered. Click the topic title to find out how to solve your problem:

How to update ESET NOD32 Antivirus
How to remove a virus from my PC
How to create a new task in Scheduler
How to schedule a scan task (every 24 hours)

If your problem is not included in the help pages list above, try searching the ESET NOD32 Antivirus help pages.

If you cannot find the solution to your problem/question in the help pages, you can visit our regularly updated online ESET Knowledgebase. Links to our most popular Knowledgebase articles are included below to help you resolve common issues:

I received an activation error while installing my ESET product. What does it mean?
How do I enter my Username and Password in ESET Smart Security/ESET NOD32 Antivirus?
I receive the message that my ESET installation ended prematurely
What do I need to do after renewing my license? (Home users)
What if I change my email address?
How to start Windows in Safe Mode or Safe Mode with networking

If necessary, you can contact our Customer Care with your questions or problems. The contact form can be found in the **Help and Support** tab of ESET NOD32 Antivirus.

7.1 How to update the ESET NOD32 Antivirus

Updating ESET NOD32 Antivirus can be performed either manually or automatically. To trigger the update, click **Update now** in the **Update** section.

The default installation settings create an automatic update task which is performed on an hourly basis. If you need to change the interval, please navigate to **Tools** > **Scheduler** (for more information on Scheduler, click here).

7.2 How to remove a virus from my PC

If your computer is showing symptoms of malware infection, e.g. it is slower, often freezes, we recommend that you do the following:

1. In the main program window, click **Computer scan**.
2. Click **Scan your computer** to begin scanning your system.
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.
4. If you wish to only scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

For additional information please see our regularly updated ESET Knowledgebase article.

7.3 How to create a new task in Scheduler

To create a new task in **Tools** > **Scheduler**, click **Add** or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** – Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** – Performs a computer scan of files and folders on your computer.
- **Update** – Schedules an Update task by updating the virus signature database and program modules.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:

From the **Scheduled task** drop-down menu, select **Update**. Enter the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered.** Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if time since last run exceeds a specified value** (the interval can be defined using the **Time since last run (hours)** scroll box)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

7.4 How to schedule a weekly computer scan

To schedule a regular task, open the main program window and click **Tools** > **Scheduler**. Below is a short guide on how to schedule a task that will scan your local drives every 24 hours. See our Knowledgebase article for more detailed instructions.

To schedule a scan task:

1. Click **Add** in the main Scheduler screen.
2. Select **On-demand computer scan** from the drop-down menu.
3. Enter a name for the task and select **Weekly** for the task frequency.
4. Set the day and time the task will execute.
5. Select **Run the task as soon as possible** to perform the task later if the scheduled task does not run for any reason (for example, if the computer was turned off).
6. Review the summary of the scheduled task and click **Finish**.
7. From the **Targets** drop-down menu, select **Local drives**.
8. Click **Finish** to apply the task.